BẢN TIN NỘI BỘ

CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Phần mềm độc hại rút tiền ATM đã lan rộng ở nhiều quốc gia

Lúc 10 giờ một ngày cuối tháng 11/2018, nhân viên ngân hàng tại Freiburg, Đức phát hiện thấy hệ thống báo cây ATM đã gặp lỗi. Vụ việc đã được trình báo lên cơ quan chức năng, theo kết quả kiểm tra, máy ATM đã bị nhiễm một loại malware có tên "Cutlet Maker", có khả năng điều khiển máy ATM trả ra tất cả tiền (hiện có) trong thiết bị. Đến nay, việc sử dụng malware Cutlet Maker để thực hiện các vụ việc tương tự đang thực sự xảy ra trên toàn thế giới chứ không chỉ ở riêng nước Đức. Việc sở hữu malware này ngày một dễ lại càng tăng tốc độ lây lan trên toàn thế giới.

Vào thời điểm vụ tấn công xảy ra tại Đức, khi đó màn hình máy ATM hiện dòng chữ " Ho-ho-ho! Let's make some cutlets today!", (có nghĩa là Ho-ho-ho! Hãy bắt tay vào làm món cutlet nào!) kèm theo đó đó là hình ảnh hoạt họa của một đầu bếp và một miếng thịt đang tươi cười. Từ "cutlet" ở đây có hai nghĩa, một là món ăn làm từ thịt, hai là tiếng lóng của người Nga có nghĩa là "một cục tiền".

Phương thức ăn cắp tiền mới này được gọi là "jackpotting", bắt đầu xuất hiện tại các máy ATM ở Đức từ năm 2017. Tổng thiệt hại trong giai đoạn này lên tới hơn một triệu Euro. Jackpotting tiên tiến hơn nhiều những cách thức ăn cắp trước đây, bởi lẽ nó không cần tới sự hiện diện của thẻ ngân hàng, tin tặc chỉ cần dùng USB để cài malware vào ATM, tất cả tiền trong máy sẽ tuôn ra.

Mới đây, trang tin Motherboard cộng tác với phóng viên Bayerischer Rundfunk tới từ Đức vừa khám phá ra thêm những tình tiết mới trong những vụ jackpotting đang xuất hiện ngày một nhiều này.

Tại hội nghị an ninh mạng Black Hat 2010, nhà nghiên cứu bảo mật quá cố Barnaby Jack đã tiến hành hack máy ATM ngay trên sân khấu bằng một loại malware do ông tự tạo ra. Màn hình máy ATM khi đó hiện ra chữ "JACKPOT" và đẩy ra một dòng tiền giấy, trước những tràng pháo tay của người xem. Còn hiện tại, loại malware này đã hiện hữu và đang lây lan ngày một rộng rãi.

Trong vụ việc xảy ra ở Freiburg đã nêu ở đầu bài viết, tin tặc đã không lấy được đồng nào. Thế nhưng theo Christoph Hebbecker, một luật sư Đức cho biết, văn phòng của ông đang theo sát một loạt vụ tương tự; từ thời điểm tháng 2 đến tháng 11/2017, đã có tổng cộng 10 vụ jackpotting diễn ra. Tổng số tiền tin tặc đã lấy được chạm mốc 1,4 triệu Euro.

Luật sư Hebbecker nói thêm rằng những vụ đánh cắp tiền này đều giống nhau, ông tin rằng chúng đều có liên quan tới một tổ chức tội phạm nào đó. Bên điều tra có thu được một vài video về hành động của kẻ gian, tuy nhiên họ chưa tìm ra được nghi phạm. Nhiều nguồn tin khác cho biết thêm những vụ tấn công máy ATM trong năm 2017 ảnh hưởng trực tiếp tới ngân hàng Santander; trong đó có những nguồn tin nêu cụ thể rằng phương pháp jackpotting ảnh hưởng tới các máy ATM mẫu Wincor 2000xe, do công ty Diebold Nixdorf sản xuất.

Thời điểm đó ngân hàng Santander cũng đã có tuyên bố chính thức, trấn an khách hàng về những vụ việc jackpotting đang diễn ra ngày một nhiều. Chính quyền thành phố Berlin cũng công bố họ đã phát hiện tổng cộng 36 vụ jackpotting tính từ mùa xuân năm 2018 và có vài ngàn Euro đã bị đánh cắp từ các máy ATM. Tuy nhiên họ không công bố cụ thể loại malware nào đã gây ra các vụ jackpotting. Tính từ ngày phương pháp ăn cắp tiền này xuất hiện, nước Đức đã có 82 vụ việc, tuy nhiên không phải vụ nào cũng thành công.

Có một điều quan trọng cần phải nhấn mạnh: đó là phương pháp jackpotting không bị giới hạn bởi ngân hàng hay mẫu máy ATM. Chắc chắn có những ngân hàng khác ngoài Santander bị ảnh hưởng và những máy ATM khác ngoài của Diebold Nixdorf bị tấn công. Nguy hiểm hơn, phương pháp này (và cũng rất có thể là malware Cutlet Maker) đã và đang có xu hướng ảnh hưởng và lan rộng trên toàn thế giới.

Một phần lỗi thuộc về phần mềm có trên những chiếc máy ATM đã cũ, chạy phần mềm cũ và chậm. Các công ty sản xuất máy ATM khẳng định đã có nhiều cải tiến bảo mật, nhưng trong thực tế vẫn còn rất nhiều máy ATM cũ vẫn đang hoạt động, tiềm ẩn nhiều rủi ro. Bên cạnh đó, không chỉ người sản xuất máy có trách nhiệm bảo vệ tài sản của mình mà các ngân hàng cũng phải chung tay trong việc này.

Cùng thời điểm các vụ jackpotting diễn ra năm 2017, các nhà nghiên cứu bảo mật tại Kaspersky đã công bố một báo cáo cho thấy phần mềm Cutlet Maker đã được rao bán trên các forum từ hồi tháng 5/2017 với giá chỉ khoảng 1000 USD. Điều này đồng nghĩa với việc Cutlet Maker có thể phát tán đi bất cứ địa phương nào, không chỉ riêng tại Châu Âu.

Nhóm phóng viên của Motherboard đã thử liên hệ với một tài khoản forum đăng tin bán Cutlet Maker. Người bán đã viết mail cho phóng viên, nói thêm rằng chỉ với 1000 USD là có thể sở hữu malwave này và họ có thể hướng dẫn cách sử dụng luôn. Họ cung cấp ảnh chụp màn hình hướng dẫn sử dụng bằng tiếng Nga và tiếng Anh, chỉ ra từng bước cần thực hiện để rút ruột một máy ATM. Trong hướng dẫn, có cả phần kiểm tra máy có bao nhiêu tiền và cách cài cắm malware vào máy.

Hiệp hội Giao dịch bảo mật châu Âu (EAST), tổ chức phi lợi nhuận chuyên theo dõi các giao dịch lừa đảo, công bố rằng các vụ việc jackpotting đã giảm 43% tính từ năm 2018 đến nay nhưng đây mới chỉ là số liệu tại Châu Âu. Việc malware ngày càng dễ tiếp cận, với giá rất rẻ so với những gì chúng mang lại sẽ khiến việc lây lan dễ dàng hơn trước nhiều. Tháng 1/2018, Mật vụ Hoa Kỳ cảnh báo các cơ quan tài chính trong nước về vụ việc jackpotting đầu tiên xuất hiện tại Mỹ, với một malware có tên Ploutus.D, chưa rõ đây là biến thể của Cutlet Maker hay là một malware hoàn toàn mới, thuộc một tổ chức jackpotting khác. Nhưng đây là một minh chứng cho việc jackpotting đang lây lan mạnh mẽ trên toàn cầu. Các tổ chức tài chính, ngân hàng và cơ quan thực thi pháp luật cần sớm có các biện pháp mạnh mẽ hơn để có thể đảm bảo an toàn tài sản của mình.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra kỹ càng trước khi sử dụng giao dịch tại cây ATM để tránh lộ lọt thông tin và mất mát tài sản.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=c74b5c11-1141-471b-95c8-a05fe6e7d3a6&NewsID=30686cbf-ce17-4ba1-b691-99e80e1fd0fe

2. Hacker Trung Quốc dùng vân tay trên cốc thủy tinh để bẻ khóa cảm biến siêu âm, điện dung lẫn quang học trong 20 phút

Bạn có chắc là muốn uống nước bằng chiếc cốc thủy tinh không? Bởi vân tay của bạn sẽ bám đầy trên thành cốc, và rõ ràng nhiêu đó là quá đủ để hacker bẻ khóa smartphone của bạn rồi.

Nhóm hacker X-Lab thuộc Tencent Security đã trình diễn kỹ thuật này tại một sự kiện hack ở Thượng Hải bằng cách mời một số khán giả chạm vào cốc. Sau đó trưởng nhóm, Chen Yu, lấy điện thoại của mình ra, chụp ảnh vân tay trên cốc, đưa nó vào ứng dụng họ mới phát triển để trích xuất dữ liệu chính xác. Dữ liệu này được dùng để tạo ra bản sao vật lý của vân tay người dùng chỉ trong vòng 20 phút.

Kết quả? Bản sao vân tay kia đã đánh lừa được 3 chiếc smartphone và 2 cỗ máy khác được trang bị máy quét vân tay.

"Để thực hiện cuộc tấn công này, cần phần cứng có giá 140 USD, và phần mềm chỉ bao gồm một điện thoại và một ứng dụng" - nhà nghiên cứu Chen Yu của X-Lab nói.

Tencent tất nhiên từ chối tiết lộ thêm thông tin về phương thức cụ thể họ đã sử dụng.

X-Lab khẳng định họ là nhóm đầu tiên bẻ khóa được cảm biến vân tay siêu âm, cùng với hai loại cảm biến vân tay khác được dùng phổ biến trên smartphone là cảm biến điện dung và cảm biến quang học.

Nhưng khẳng định này không hoàn toàn đúng. Cảm biến vân tay siêu âm trên Galaxy S10 thực ra đã bị bẻ khóa vào đầu tháng này bởi một phụ nữ ở Anh, bằng một miếng dán màn hình giá 3,4 USD mua trên eBay.

Công ty Hàn Quốc sau đó đã tung ra một bản vá cho cảm biến vân tay của Galaxy S10 và Note 10, nhưng đã quá muộn ở Trung Quốc vì cả WeChat Pay và Alipay - hai nền tảng thanh toán di động lớn nhất nước này - đều đã ngừng kích hoạt việc sử dụng cảm biến vân tay trên một số thiết bị Samsung để xác thực giao dịch.

Được phát triển bởi Qualcomm, cảm biến vân tay siêu âm được quảng cáo là một giải pháp đáng tin cậy hơn và nhanh hơn so với các cảm biến vân tay trong màn hình khác. Chúng phát sóng âm thanh đến ngón tay bạn và dựa vào dữ liệu dội ngược lại để tạo nên hình ảnh 3 chiều về vân tay. Xiaomi cũng đã sử dụng cảm biến vân tay siêu âm trên một số thiết bị của hãng.

Năm ngoái, nhóm của Chen đã phát hiện ra một lỗi thiết kế ảnh hưởng đến các cảm biến vân tay trong màn hình thế hệ cũ hơn, khiến nửa tá smartphone đứng trước nguy cơ, bao gồm cả Huawei Mate 20 Pro. Điều duy nhất cần để thực hiện cuộc tấn

công là một vật liệu phản chiếu mờ đục. Nếu bạn đang tự hỏi thứ đó có thể tìm thấy ở đâu, thì bạn sẽ há hốc mồm khi biết nó thực ra khá phổ biến: giấy nhôm.

Một nhóm nghiên cứu bảo mật khác của Tencent, Keen Lab, đã phát hiện nhiều lỗi trong hệ thống hỗ trợ lái xe tiên tiến của Tesla trong năm nay, đánh lừa một chiếc Model S lấn sang làn đối diện.

Trong lần hack mới nhất này, các nhà nghiên cứu X-Lab cho biết họ đã phát triển ứng dụng trong nhiều tháng. Họ còn để ý thấy rằng việc trích xuất một dấu vân tay từ mặt kính điện thoại thậm chí dễ dàng hơn nhiều so với từ một chiếc cốc thủy tinh.

Nhưng X-Lab nói rằng bạn không nên quá lo lắng về vấn đề này. Chen cho biết bạn chỉ cần nhớ lau sạch vân tay thường xuyên bất kỳ khi nào chạm vào thứ gì đó.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần luôn đề cao cảnh giác khi sử dụng hình thức bảo mật sinh trắc học như cảm biến vân tay, gương mặt; mặc dù kém tiện lợi hơn nhưng sử dụng mã PIN và mật khẩu là hình thức bảo mật tốt hơn.

Link tham khảo: http://genk.vn/hacker-trung-quoc-dung-van-tay-tren-coc-thuy-tinh-de-be-khoa-cam-bien-sieu-am-dien-dung-lan-quang-hoc-trong-20-phut-20191028231208957.chn

3. Lỗ hổng mới trong PHP khiến các web chạy máy chủ NGINX bị hack

Nếu người dùng đang chạy bất kỳ website nào sử dụng nền tảng PHP trên máy chủ NGINX và có bật tính năng PHP-FPM nhằm mang lại hiệu suất tốt hơn thì hãy cẩn thận với một lỗ hổng được tiết lộ gần đây có thể khiến tin tặc tấn công máy chủ website từ xa.

Lỗ hổng được định danh CVE-2019-11043 ảnh hưởng đến các wesbite có cấu hình PHP-FPM nhất định không hiếm gặp trên thực tế và có thể dễ dàng bị khai thác vì mã khai thác (PoC) cho lỗ hổng này đã được công bố công khai.

PHP-FPM là viết tắt của FastCGI Process Manager cung cấp các tính năng giúp tối ưu quá trình xử lý thông tin nhằm tăng tốc độ các website viết bằng ngôn ngữ lập trình PHP.

Lỗ hổng chính nằm ở biến env_path_info trong module PHP-FPM, biến đó khi bị tràn số sẽ có thể khai thác và cho phép kẻ tấn công thực thi lệnh từ xa trên máy chủ web.

Những website nào tiềm ẩn nguy cơ bị khai thác từ lỗ hổng trên?

Qua mã khai thác được công bố, việc khai thác này nhằm vào các máy chủ chạy các phiên bản PHP 7+, lỗi underflow PHP-FPM cũng ảnh hưởng đến các phiên bản PHP trở về trước.

Cụ thể, một website có thể dính lỗ hổng này, nếu:

NGINX được cấu hình đề chuyển tiếp yêu cầu của các trang PHP đến PHP-EPM xử lý

fastcgi_split_path_info directive tồn tại trong cấu hình và bao gồm một biểu thức chính quy bắt đầu bằng ký tự '^' và kết thúc bằng ký tự '$'

Biến PATH_INFO được định nghĩa với fastcgi_param directive

Không có kiểm tra như 'try_files $uri =404' hoặc if (-f $uri) nhằm xác định liệu một file có tồn tại không

Lỗ hổng thực thi code trên PHP FPM hoạt động như thế nào?

Theo các nhà nghiên cứu, biểu thức chính quy trong 'fastcgi_split_path_info' directive có thể bị phá vỡ bằng bằng cách sử dụng ký tự tạo dòng mới (newline character) %0a. Biểu thức chính quy bị phá vỡ dẫn đến PATH_INFO rỗng, gây ra lỗi.

Đoạn sau trong mã nguồn, giá trị path_info[0] được đặt thành 0, sau đó FCGI_PUTENV được gọi. Sử dụng một URL với đường dẫn và chuỗi truy vấn có độ dài được lựa chọn cẩn thận, kẻ tấn công có thể làm cho path_info trỏ chính xác đến byte đầu tiên của _fcgi_data_seg structure. Đặt 0 vào nó di chuyển trường 'char* pos' về sau, và tiếp theo FCGI_PUTENV ghi đè một số dữ liệu (bao gồm các biến fast cgi khác) với đường dẫn của script. Sử dụng kỹ thuật này nhà nghiên cứu có thể tạo một biến fcgi PHP_VALUE giả và sau đó sử dụng một chuỗi các giá trị cấu hình được lựa chọn cẩn thận để thực thi code.

Bản cập nhật PHP 7 đã được phát hành để vá lỗ hổng FPM

Danh sách các điều kiện tiên quyết để khai thác lỗ hổng thành công như đã đề cập ở trên không phải là hiếm bởi các cấu hình có lỗ hổng được một số nhà cung cấp máy chủ web sử dụng và sẵn có trên mạng là một phần trong nhiều hướng dẫn về PHP FPM.

Một trong những nhà cung cấp dịch vụ máy chủ web là Nextcloud, đã phát đi cảnh báo người dùng các cấu hình Nextcloud NGINX mặc định cũng có thể bị tấn công và khuyến cáo quản trị hệ thống cập nhật bản vá ngay lập tức.

Vì mã khai thác lỗ hổng này được công bố và bản vá chỉ mới được phát hành gần đây nên những kẻ tấn công có thể bắt đầu quét mạng nhằm tìm kiếm các wesbite dính lỗ hổng.

Người dùng được khuyến cáo ngay lập tức cập nhật lên phiên bản PHP 7.3.11 và PHP 7.2.24 mới nhất kể cả khi không sử dụng cấu hình có lỗ hổng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần cập nhật các bản vá mới nhất của PHP để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-moi-trong-php-khien-cac-web-chay-may-chu-nginx-bi-hack.12873/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Android	CVE-2019-2186 CVE-2019-2185 CVE-2019-2184 …	Nhóm 08 lỗ hổng trên một số thành phần của hệ điều hành Android cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa mà không cần quyền thực thi, thu thập thông tin (user và mật khẩu người dùng).	Đã có thông tin xác nhận và bản vá.
2	Linux	CVE-2019-17351 CVE-2019-17133 CVE-2019-17075 …	Nhóm 10 lỗ hổng trên hệ điều hành Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
3	D-Link	CVE-2019-17508 CVE-2019-17506 CVE-2017-14948	Nhóm 08 lỗ hổng trên một số sản phẩm của D-Link (DAP-1320 A2-V1.21, DIR-412 A1-1.14WW, DIR-866L 1.03B04, DIR-816 A1 1.06…) cho phép đối tượng tấn công khai thác lỗi XSS,thu thập thông tin về hệ thống mạng, đánh cắp thông tin xác thực, chèn và thực thi mã lệnh từ đó kiểm soát thiết bị	Một số lỗ hổng đã có thông tin xác nhận và bản vá
4	Cisco	CVE-2019-15259 CVE-2019-15256 CVE-2019-12707 …	Nhóm 41 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Aironet Access Points, Catalyst 9100 Access Points, Unified Communications Manager, Firepower Management Center…) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau gồm thu thập thông tin, thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
5	WordPress	CVE-2019-17386 CVE-2019-17672 CVE-2015-9490	Nhóm 25 lỗ hổng trên một số thành phần, phiên bản của WordPress cho phép đối tượng tấn công thu thập thông tin	Một số lỗ hổng đã có thông tin xác nhận và

			người dùng trên hệ thống (user_login, user_pass, user_email values), khai thác lỗi XSS, SSRF,	bản vá
6	Oracle	CVE-2019-2937 CVE-2019-2971 CVE-2019-2901	Nhóm 136 lỗ hổng trên một số sản phẩm của Oracle (Oracle Outside In Technology, Oracle Jdeveloper&ADF, Database Server, E-Business Suite...) cho phép đối tượng tấn công truy cập trái phép vào ứng dụng trên hệ thống, tấn công từ chối dịch vụ, sửa đổi trái phép dữ liệu,	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	soplifan.ru
5	xjpakmdcfuqe.com
6	xdqzpbcgrvkj.ru
7	hjb343e8.ru
8	rkphklelf.ru
9	cp.hfuabnqx.ru
10	morphed.ru

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
   - Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
   - Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.