BẢN TIN NỘI BỘ

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

1. Tấn công DDoS vẫn tăng trong quý 2

Theo đó, số vụ tấn công DDoS trong quý 2/2019 giảm hơn 44% so với quý 1/2019. Điều này không nằm ngoài dự đoán vì các cuộc tấn công DDoS thường không diễn ra mạnh thời điểm cuối mùa xuân và mùa hè. Tuy nhiên, số lượng các cuộc tấn công DDoS trong quý 2/2019 vẫn tăng 18% so với quỳ 2/2018 và tăng 25% so với quý 2/2017.

Số lượng tấn công tầng ứng dụng không bị tác động đáng kể bởi xu hướng giảm tấn công DDoS theo mùa, với tỷ lệ giảm chỉ 4% so với quý trước. Những kiểu tấn công này nhắm vào các tính năng hoặc ứng dụng API nhất định để phá hủy không chỉ mạng mà còn cả tài nguyên máy chủ. Ngoài ra, chúng cũng khó bị phát hiện và ngăn chặn hơn, vì chúng ẩn dưới các yêu cầu hợp pháp.

Số lượng tấn công tầng ứng dụng đã tăng gần 32% so với quý 2/2018 và chiếm 46% trong tổng số các cuộc tấn công DDoS trong quý 2/2019. Tỷ lệ số lượng tấn công tầng ứng dụng trong tổng lượng tấn công DDoS vào quý 2/2019 tăng 9% so với quý 1/2019 và tăng 15% so với quý 2/2018.

Theo số liệu thống kê qua các botnet sử dụng hệ thống Kaspersky DDoS Intelligence, tổng số vụ tấn công DDoS tại Việt Nam đã tăng nhẹ từ 108 vào quý 2/2018 lên 114 vào quý 2/2019.

Phân tích các lệnh mà botnet nhận được từ cơ sở hạ tầng chỉ huy và kiểm soát (C&C) cho thấy cuộc tấn công DDoS dài nhất trong quý 2/2019 kéo dài 509 giờ - gần 21 ngày. Đây là cuộc tấn công dài nhất kể từ khi Kaspersky bắt đầu theo dõi hoạt động botnet vào năm 2015. Trước đó, cuộc tấn công dài nhất kéo dài 329 giờ được thực hiện vào quý 4/2018.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần luôn đề cao cảnh giác trước những khả năng bị tấn công DDoS hiện nay để đảm bảo an toàn thông tin cho hệ thống.

Link tham khảo: https://thanhnien.vn/cong-nghe/tan-cong-ddos-van-tang-trong-quy-2-1111766.html

2. Lỗ hổng BlueKeep đe dọa hơn 800 nghìn hệ thống

BlueKeep là một lỗ hổng thực thi mã từ xa trong Dịch vụ kết nối Máy tính từ xa của Windows (Windows Remote Desktop Services), cho phép tin tặc kiểm soát toàn quyền một máy tính. Lỗ hổng này ảnh hưởng đến các máy tính sử dụng hệ điều hành từ Windows XP đến Windows 7 và Windows Server 2003 đến Server 2008 R2.

Lỗ hổng BlueKeep có định danh CVE-2019-0708, được đánh giá mức độ nghiêm trọng. Đáng lo ngại, tin tặc có thể sử dụng lỗ hổng như một phương thức để phát tán mã độc đào tiền ảo, trojan ngân hàng hoặc các loại mã độc khác, mà không cần sự tương tác của người dùng.

Theo thống kê của công ty an ninh mạng BitSight (có trụ sở chính tại Mỹ), tính đến ngày 02/7 vẫn tồn tại 805.665 hệ thống bị ảnh hưởng (giảm 17% so với ngày 31/5). Ước tính trung bình mỗi ngày giảm 5.224 số lượng hệ thống bị ảnh hưởng. Bằng cách theo dõi các hệ thống riêng lẻ vẫn tồn tại lỗ hổng và kết nối với Internet, sau đó xác định thời điểm chúng được cập nhật bản vá, công ty này có thể ước tính, trung bình ít nhất 854 hệ thống được vá mỗi ngày. Sự chênh lệch giữa hai ước tính này thể hiện số lượng hệ thống không còn tiếp xúc với dịch vụ Internet hoặc các hệ thống thay đổi địa chỉ IP thường xuyên.

Trung Quốc và Mỹ là những quốc gia có số lượng hệ thống bị ảnh hưởng nhiều nhất, mặc dù cả hai đều có mức giảm mạnh nhất trên toàn cầu lần lượt là 24% và 20%.

Các lĩnh vực có mức độ giảm số lượng hệ thống bị ảnh hưởng nhiều nhất trên thế giới là ngành pháp lý (33%), các tổ chức phi lợi nhuận/ phi chính phủ (27%) và hàng không vũ trụ/ quốc phòng (24%). Trái lại, những ngành có mức giảm ít nhất là tiêu dùng (5%), tiện ích công cộng (10%) và công nghệ (12%).

BitSight cũng đưa ra cảnh báo, các tổ chức nên có cách tiếp cận chủ động hơn đối với các bên thứ ba có thể chịu ảnh hưởng bởi lỗ hổng BlueKeep. Công ty cho biết thêm, có nhiều cách để quản trị viên hệ thống khắc phục việc ảnh hưởng đến các hệ thống bên ngoài. Việc đầu tiên và quan trọng nhất chính là cập nhật bản vá cho hệ thống bị ảnh hưởng, bởi Microsoft đã phát hành bản vá cho lỗ hổng này được 02 tháng. Ngoài ra, có thể loại bỏ kết nối với Internet, hoặc áp dụng danh sách kiểm soát truy cập phù hợp để hạn chế quyền truy cập tới các hệ thống bị ảnh hưởng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần thường xuyên kiểm tra và tải về các bản cập nhật của hệ điều hành để đảm bảo an toàn thông tin.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?NewsID=fbd63db9-19cf-4e86-9185-7105726bfda0&CatID=a36fcc1c-e27c-4424-82c8-622de7fa7f9a&MenuID=222f9fad-ff28-43b9-8fe3-0612c407cc72

3. Twitter xuất hiện "lỗi" khiến thông tin người dùng bị nhà cung cấp quảng cáo bên thứ 3 tiếp cận

Mới đây, một blog vi mô của Twitter đã chính thức tiết lộ thông tin rằng một số đối tác quảng cáo bên thứ 3 đã cố gắng lạm dụng một lỗ hổng trong trong hệ thống của nền tảng truyền thông xã hội này nhằm trích xuất thông tin người dùng mà không có sự đồng ý của chủ tài khoản. Đây có thể được coi là hành vi vi phạm dữ liệu nội bộ tương đối nghiêm trọng.

Hiện lỗ hổng này đã được vá thành công vào ngày 5 tháng 8 năm 2019, chưa có bất cứ thiệt hại đáng kể nào được ghi nhận. Twitter cam kết với người dùng rằng họ sẽ theo dõi sát sao vụ việc và gửi thông báo chi tiết về tình hình thực tế cho tất cả các tài khoản bị ảnh hưởng bởi hành vi thu thập dữ liệu trái phép của nhà cung cấp quảng cáo bên thứ 3. Thông báo chính thức của @TwitterSupport như sau:

"Một lỗi bảo mật nhỏ xuất hiện trên nền tảng Twitter cho iOS đã vô tình cho phép các nhà cung cấp quảng cáo bên thứ 3 thu thập và chia sẻ dữ liệu vị trí của người dùng. Chúng tôi hiện đã vá lỗi, và đảm bảo sẽ cung cấp chi tiết mọi thông tin liên quan đến vụ việc cho các tài khoản bị ảnh hưởng".

Theo điều tra, sự tồn tại của lỗ hổng này đã được một số đối tác quảng cáo của Twitter biết đến lần đầu tiên kể từ tháng 5 năm 2018, nhưng Twitter đã không có những biện pháp xử lý cần thiết. Thời điểm đó, trang blog vi mô vẫn chưa nắm rõ chi tiết cụ thể về vụ việc.

Dữ liệu vị trí của mỗi tài khoản thường được Twitter lưu trữ "an toàn" trong cơ sở dữ liệu người dùng như một phần của chính sách bảo mật dữ liệu, nhưng trên thực tế, chưa thể khẳng định rằng liệu các nhà quảng cáo đối tác của trang mạng xã hội này có được cấp quyền truy cập vào kho dữ liệu đó hay không.

Dữ liệu vị trí của người dùng thường được sử dụng cho quy trình khôi phục tài khoản, và không được thiết kế, đồng thời cũng không phải là một loại "hàng hóa" có thể được phép "bán" cho các nhà quảng cáo. Tuy nhiên kết quả điều tra cho thấy khi tài khoản người dùng Twitter bị ảnh hưởng bởi lỗ hổng nêu trên, việc trích xuất dữ liệu vị trí thậm chí còn có thể được thực hiện tùy ý bởi một đối tác quảng cáo của Twitter ngay cả khi người dùng không đồng ý (đa số là không hề hay biết).

Cách đây hơn 1 năm, Ủy ban Châu Âu (EC) đã cho ban hành và thực thi một cách quyết liệt Quy định bảo vệ dữ liệu chung (GDPR) đối với mọi quốc gia thành viên EU, cũng như tất cả các công ty đã và đang phục vụ công dân EU kể từ ngày 25 tháng 5 năm 2018. Rất nhiều ông lớn trong lĩnh vực cung cấp dịch vụ internet đã bị "sờ gáy", bao gồm Facebook, Google, và cả Microsoft. Hàng tỷ đô la tiền phạt đã được áp dụng, và nếu vụ vi phạm dữ liệu trên được chứng minh là bắt nguồn từ lỗi chủ quan của Twitter và có liên quan đến công dân EU, một án phạt nặng rất có thể sẽ được áp dụng. Đã phải mất tới hơn một năm để xác nhận sự tồn tại của lỗ hổng, và trong đó chắc chắn bao gồm thông tin tài khoản của một công dân EU.

"Chúng tôi có thể đã hiển thị cho bạn các quảng cáo dựa trên những suy luận liên quan đến thiết bị mà bạn sử dụng ngay cả khi chưa hỏi ý kiến. Tuy nhiên đây chỉ là một phần trong quá trình thử nghiệm thuật toán nhằm đưa ra quảng cáo phù hợp hơn cho người dùng Twitter và các dịch vụ khác của chúng tôi kể từ tháng 9 năm 2018" đội ngũ Twitter giải thích.

Các cuộc điều tra vẫn đang tiếp tục và nhắm đến các nhóm phụ trách công nghệ bên trong và bên ngoài trang mạng xã hội này để xác định toàn bộ phạm vi tác động của lỗ hổng, thậm chí cả đối tác của Twitter cũng nằm trong tầm ngắm.

Về phần mình, Twitter cam kết rằng bất kỳ phát hiện mới nào cũng đều sẽ được tiết lộ công khai ngay lập tức, không có ngoại lệ.

Người dùng Twitter nếu muốn liên hệ với đại diện trang mạng xã hội này để cập nhật thêm thông tin cụ thể đều có thể sử dụng biểu mẫu tùy chỉnh mà công ty cung cấp. Tất cả vẫn còn đang trong quá trình điều tra và chúng tôi sẽ thông báo đến bạn ngay khi có thông tin mới nhất.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng mạng xã hội cần đề cao cảnh giác, không đưa những thông tin quan trọng nhạy cảm lên mạng xã hội.

Link tham khảo: https://quantrimang.com/twitter-xuat-hien-loi-khien-thong-tin-nguoi-dung-bi-tiep-can-165867

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	Cpanel	CVE-2019-14408 CVE-2018-20863 CVE-2018-20869 ...	Nhóm 249 lỗ hổng trên cpanel - ứng dụng phổ biến sử dụng để quản lý web, cho phép đối tượng tấn công khai thác lỗi SQL Injection, XSS, chèn và thực thi mã lệnh qua nhiều thành phần khác nhau, tấn công leo thang.	Đã có thông tin xác nhận và bản vá.
2	EspoCRM	CVE-2019-14329 CVE-2019-14330 CVE-2019-14349 …..	Nhóm 06 lỗ hổng trên phần mềm EspoCRM - phần mềm quản lý khách hàng cho phép đối tượng tấn công khai thác lỗi XSS qua nhiều thành phần khác nhau, thực hiện tấn công vét cạn để đánh cắp thông tin tài khoản.	Một số lỗ hổng đã có cách khắc phục.
3	Jenkins	CVE-2019-10356 CVE-2019-10362 CVE-2019-10344 ...	Nhóm 14 lỗ hổng trên một số plugin của Jenkins (phần mềm nguồn mở cho phép xây dựng và triển khai tự động ứng dụng, dùng nhiều trong phát triển phầm mềm) cho phép đối tượng tấn công khai thác lỗi XSS, thu thập thông tin xác thực do lưu trữ không mã hóa, truy cập trái phép vào dữ liệu trên hệ thống, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
4	D-Link	CVE-2019-14334 CVE-2019-14336 CVE-2019-14333 …	Nhóm 08 lỗ hổng trên một số sản phẩm của D-Link cho phép đối tượng tấn công thực hiện khai thác lỗi XSS, thu thập thông tin xác thực, lấy thông tin cấu hình của thiết bị, một số lỗ hổng cho phép chèn và thực thi lệnh nguy hiểm	Đã có thông tin xác nhận và bản vá

5	Elastic	CVE-2019-7615 CVE-2019-7614 CVE-2019-7616	Nhóm 03 lỗ hổng trên sản phẩm của Elastic gồm Elasticsearch, Kibana và APM agent cho phép đối tượng tấn công thực hiện tấn công nghe lén, khai thác lỗi SSRF, truy cập dữ liệu nhạy cảm của người dùng khác trên cùng hệ thống.	Chưa có thông tin xác nhận bản vá.
6	IBM	CVE-2019-4062 CVE-2019-4275 CVE-2019-4285 …	Nhóm 07 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (i2 Intelligent Analyis Platform, Jazz for Service Management, Spectrum Protect for Enterprise Resource Planning, BM WebSphere Application Server) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, lấy thông tin mật khẩu ở dạng rõ.	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	differentia.ru
2	disorderstatus.ru
3	atomictrivia.ru
4	soplifan.ru
5	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	25hj1urb.ru
7	somicrososoft.ru
8	xjpakmdcfuqe.com
9	uaqbzunani.info
10	www.cityofangelsmagazine.com

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.