Microsoft

Quan điểm sâu sắc về các lỗ hổng phần mềm, công cụ khai thác, mã độc, phần mềm tiềm ẩn không mong muốn và trang web có hại

Báo cáo Điều tra An ninh mạng của Microsoft

Tập 15

Tháng 1 đến Tháng 6 năm 2013

TÓM TẮT CÁC ĐIỂM CHÍNH

Báo cáo Điều tra An ninh mạng của Microsoft

Báo cáo Điều tra An ninh mạng của Microsoft, Tập 15

Tập 15 của *Báo cáo Điều tra An ninh mạng của Microsoft® (SIRv15)* cung cấp quan điểm chuyên sâu về các lỗ hổng phần mềm trong các phần mềm của Microsoft và bên thứ ba, công cụ khai thác, các mối đe dọa về mã độc hại và các phần mềm không mong muốn tiềm ẩn. Microsoft đã xây dựng những quan điểm này dựa trên các phân tích chi tiết theo xu hướng trong một vài năm qua, tập trung vào nửa đầu năm 2013.

Tài liệu này mô tả các điểm chính của báo cáo.

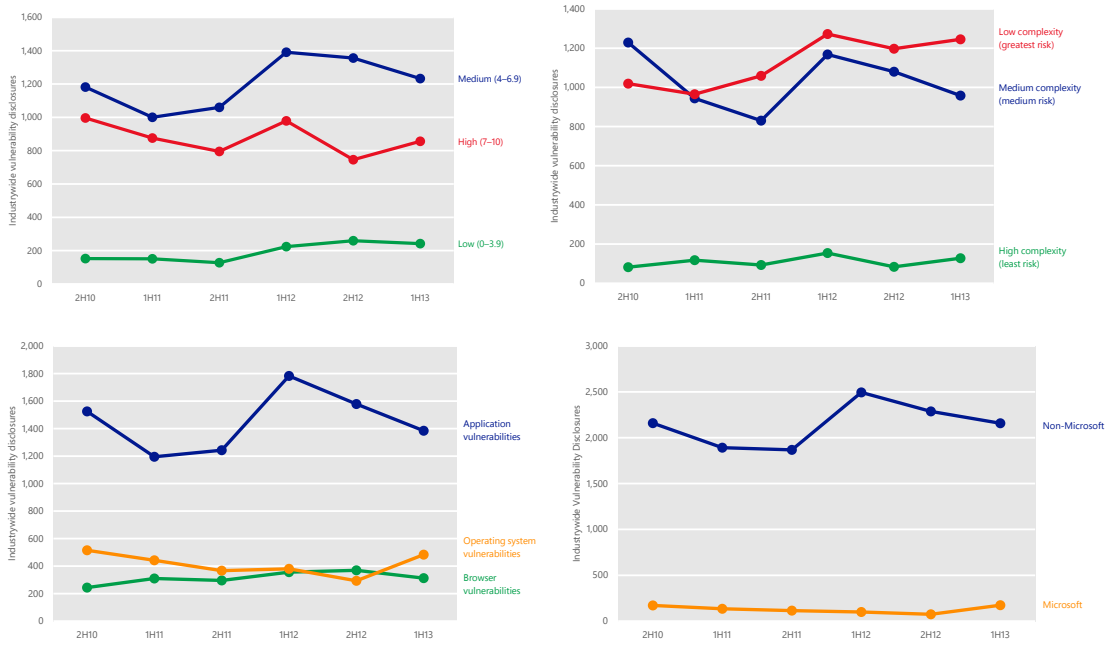
Trang web SIR cũng cung cấp phân tích chuyên sâu về các xu hướng được phát hiện tại trên 100 quốc gia/vùng trên thế giới và đưa ra các gợi ý nhằm giúp quản lý rủi ro đối với tổ chức, phần mềm và nhân viên của bạn.

Bạn có thể tải *SIRv15* về từ www.microsoft.com/sir.

Lỗ hổng

Lỗ hổng là các điểm yếu trong phần mềm cho phép kẻ tấn công phá hoại sự toàn vẹn, độ sẵn sàng hoặc bảo mật của phần mềm hoặc dữ liệu do phần mềm xử lý. Một số lỗ hổng nguy hiểm nhất cho phép kẻ tấn công khai thác hệ thống bị xâm phạm bằng cách khiến hệ thống chạy các mã độc hại mà người dùng không hề biết.

Hình 1. Các xu hướng về mức độ nghiêm trọng của lỗ hổng (CVE), sự phức tạp của lỗ hổng, phát hiện theo loại hình, và phát hiện đối với sản phẩm của Microsoft và không phải của Microsoft, trong toàn bộ ngành công nghiệp phần mềm, 2H10-1H13[1]



[1] Trong suốt báo cáo, các khoảng thời gian nửa năm và hàng quý được tham chiếu bằng định dạng nHyy hoặc nQyy, trong đó yy biểu thị năm dương lịch và n biểu thị nửa năm hoặc quý. Ví dụ: 1H13 biểu thị nửa đầu năm 2013 (từ 1 tháng 1 đến 30 tháng 6) và 4Q12 biểu thị quý thứ tư của năm 2013 (từ 1 tháng 10 đến 31 tháng 12).

- Các phát hiện về lỗ hổng trên toàn ngành đã giảm 1,3% từ 2H12, và 10,1% từ 1H12. Sự gia tăng về các phát hiện lỗ hổng của hệ điều hành trong 1H13 đã bù trừ phần lớn cho sự giảm sút tương ứng trong các phát hiện về lỗ hổng của ứng dụng trong cùng khoảng thời gian, việc này dẫn tới sự thay đổi nhr trên tổng thể. Tuy nhiên, nhìn chung các phát hiện lỗ hổng vẫn thấp đáng kể so với trước năm 2009, khi có tổng số lỗ hổng trên 3.500. Số lỗ hổng phát hiện trong một khoảng thời gian nửa năm qua là những lỗ hổng không phổ biến.

Tỷ lệ phát hiện: Giới thiệu hệ thống đo lường mới để phân tích mức độ phổ biến của phần mềm độc hại

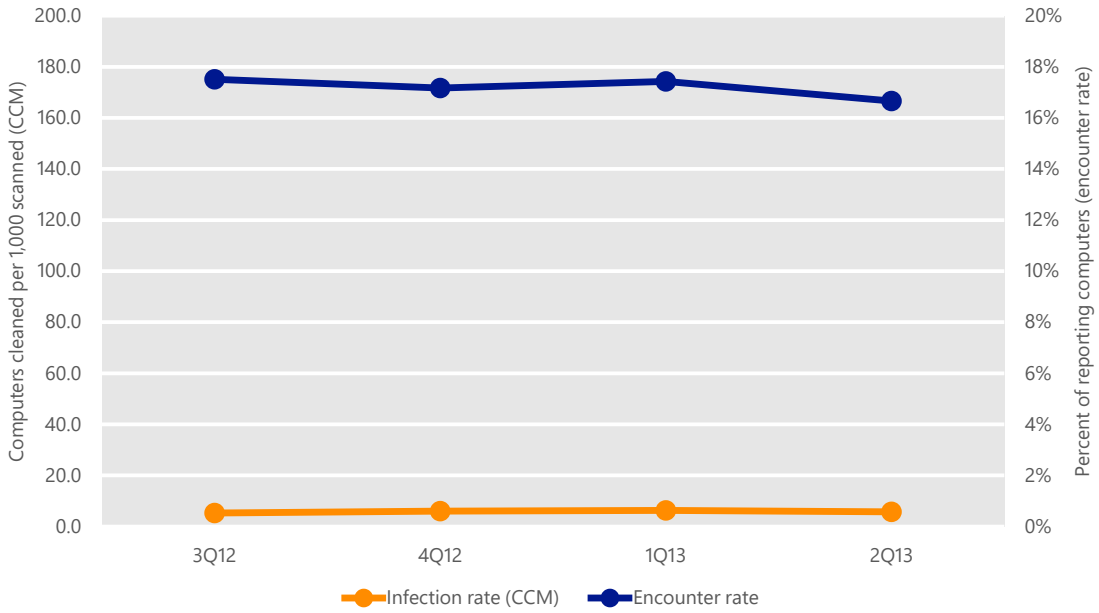
Trong một số năm, Báo cáo Điều tra An ninh mạng của Microsoft đã thông báo tỷ lệ nhiễm bằng hệ thống đo lường được gọi là tỷ lệ phần nghìn máy tính được làm sạch (CCM). CCM biểu thị số lượng máy tính được làm sạch trong mỗi 1.000 lần thực thi Công cụ Xóa Phần mềm Độc hại (MSRT). MSRT cung cấp tầm nhìn về phạm vi lây nhiễm của các dòng phần mềm độc hại cụ thể. Phạm vi tiếp cận toàn cầu, cơ sở cài đặt lớn và việc phát hành theo lịch trình thường xuyên của công cụ đã hỗ trợ việc so sánh nhất quán về tỷ lệ nhiễm tương đối giữa các quần thể máy tính khác nhau.

Để mô tả rõ hơn tất cả những gì người dùng đối mặt trong hệ sinh thái phần mềm độc hại, Microsoft đang giới thiệu một hệ thống đo lường mới có tên là tỷ lệ phát hiện. Hệ thống đo lường này là phần trăm các máy tính đang chạy các sản phẩm bảo mật thời gian thực của Microsoft phát hiện phần mềm độc hại trong khoảng thời gian cụ thể, chẳng hạn như trong một quý. Lưu ý rằng máy tính đang phát hiện phần mềm độc hại không nhất thiết bị xâm phạm bởi mối đe dọa; sản phẩm bảo mật thời gian thực có thể phát hiện mối đe dọa và ngăn chặn nó xảy ra. Việc phát hiện này sẽ được tính vào tỷ lệ phát hiện, chứ không phải tỷ lệ nhiễm cho máy tính đó.

Tỷ lệ nhiễm cùng với tỷ lệ phát hiện có thể tạo nên bức tranh toàn diện hơn về quy mô của phần mềm độc hại. Các quan điểm khác cho rằng hai hệ thống đo lường này có thể cung cấp bức tranh rõ ràng hơn về mức độ phổ biến của phần mềm và ảnh hưởng tiềm ẩn đến phạm vi toàn cầu.

Hình 2 biểu thị tỷ lệ nhiễm trên toàn thế giới so với tỷ lệ p trong từng quý từ 3Q12 đến 2Q13, với quy mô được cân bằng cho mục đích so sánh (100 trên một nghìn tương ứng với 10 phần trăm).

Hình 2. Tỷ lệ phát hiện và tỷ lệ nhiễm trên toàn thế giới, 3Q12–2Q13, theo quý



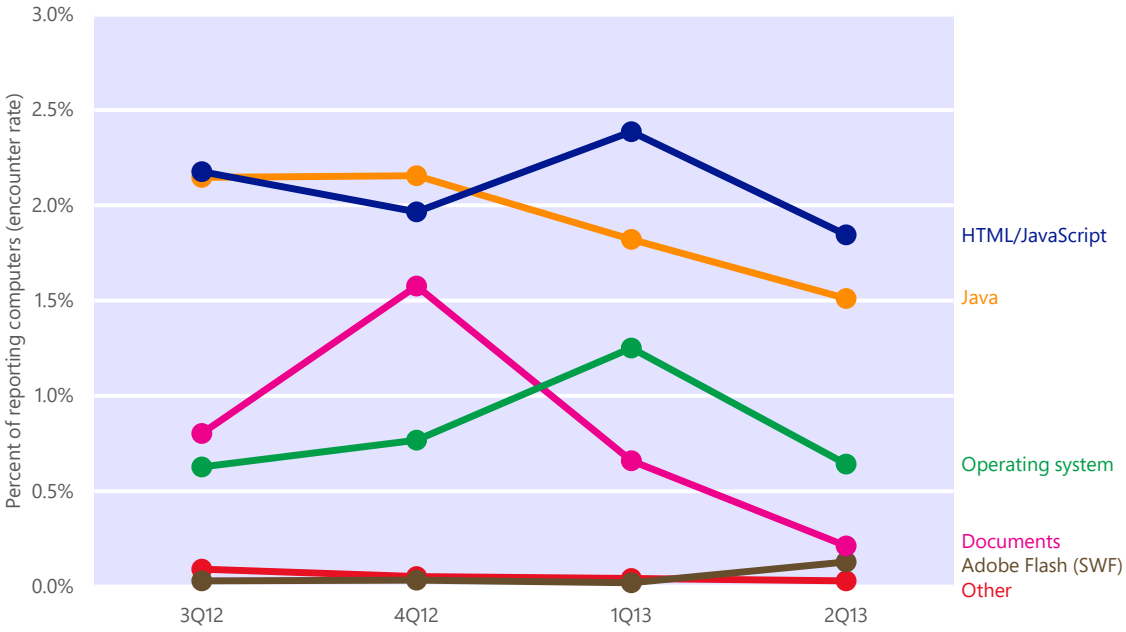
Như Hình 2 biểu thị, và đúng như kỳ vọng, tỷ lệ phát hiện phần mềm độc hại phổ biến hơn nhiều so với tỷ lệ nhiễm. Tính trung bình, khoảng 17% các máy tính trên toàn thế giới đã phát hiện phần mềm độc hại trong mỗi quý trong 1H12, theo báo cáo từ các sản phẩm bảo mật của Microsoft. Cùng thời gian đó, MSRT đã phát hiện và xóa phần mềm độc hại khỏi khoảng 6 máy tính trong mỗi 1.000 máy (0,6%).

Khai thác

Công cụ *khai thác* là mã độc hại tận dụng các lỗ hổng phần mềm để lây nhiễm, làm gián đoạn hoặc chiếm quyền kiểm soát máy tính mà không có sự đồng ý của người dùng và thường là người dùng không hề hay biết. Công cụ khai thác nhắm đến các lỗ hổng trong hệ điều hành, trình duyệt web, ứng dụng hoặc các cấu phần phần mềm được cài đặt trên máy tính. Để biết thêm thông tin, hãy tải về *SIRv15* tại www.microsoft.com/sir.

Hình 3 biểu thị mức độ phổ biến của các loại hình khai thác khác nhau được các sản phẩm chống phần mềm độc hại của Microsoft phát hiện trong mỗi quý từ 3Q12 đến 2Q13, theo số lượng máy tính riêng lẻ phát hiện.

Hình 3Các máy tính riêng lẻ báo cáo các loại nỗ lực khai thác khác nhau, 3Q12–2Q13



- Số lần phát hiện các vụ khai thác riêng lẻ thường tăng và giảm đáng kể giữa các quý khi những nhà phân phối bộ công cụ khai thác bổ sung và loại bỏ các công cụ khai thác khác nhau khỏi bộ công cụ của họ. Sự biến thiên này cũng có thể có tác động

đến mức độ phổ biến tương đối của các loại hình khai thác khác nhau, như minh họa trong Hình 3.

- Các mối đe dọa trên web (HTML/JavaScript) tiếp tục là loại hình khai thác phát hiện phổ biến nhất trong 2Q13, tiếp theo là khai thác Java và khai thác hệ điều hành. Tỷ lệ phát hiện cho khai thác HTML/JavaScript đạt cao nhất trong 1Q13, chủ yếu do dòng công cụ khai thác đa nền tảng Blacole, đã có 1,12% các máy tính trên toàn thế giới phát hiện trong quý này. (Thông tin thêm về Blacole được cung cấp trong phần tiếp theo.)

Các dòng công cụ khai thác

Hình 4 liệt kê các dòng công cụ khai thác được phát hiện nhiều nhất trong nửa đầu năm 2013.

Hình 4. Xu hướng tỷ lệ phát hiện đối với cá dòng công cụ khai thác hàng đầu do các sản phẩm chống phần mềm độc hại của Microsoft phát hiện trong 1H13, được tô màu theo mức độ phổ biến tương đối

Khai thác	Nền tảng hoặc công nghệ	3Q12	4Q12	1Q13	2Q13
HTML/IframeRef*	HTML/JavaScript	0.37%	0.58%	0.98%	1.08%
Blacole	HTML/JavaScript	1.60%	1.34%	1.12%	0.62%
CVE-2012-1723	Java	0.84%	1.32%	0.89%	0.61%
CVE-2010-2568 (MS10-046)	Hệ điều hành	0.51%	0.57%	0.57%	0.53%
CVE-2012-0507	Java	0.91%	0.53%	0.49%	0.31%
CVE-2013-0422	Java	—	—	0.38%	0.33%
CVE-2011-3402 (MS12-034)	Hệ điều hành	—	0.11%	0.62%	0.04%
Pdfjsc	Tài liệu	0.77%	1.56%	0.53%	0.12%
CVE-2013-0431	Java	—	—	0.10%	0.32%
CVE-2010-0840	Java	0.31%	0.17%	0.18%	0.21%

Các tổng không loại trừ các khai thác được phát hiện như một phần của bộ công cụ khai thác.
*Các tổng chỉ bao gồm các biến thể IframeRef được phân loại là khai thác.

- HTML/IframeRef, khai thác phát hiện phổ biến nhất trong 1H13, là sự phát hiện chung đối với các thẻ khung nội tuyến HTML (IFrame) được tạo hình đặc biệt để chuyển hướng hoặc đến các trang web từ xa chứa nội dung độc hại. Những trang độc hại này, chính xác hơn được gọi là trình tải về khai thác chứ không phải là công cụ khai thác thực sự, sử dụng nhiều kỹ thuật để khai thác các lỗ hổng trong trình duyệt và trình cắm; điểm chung duy nhất là kẻ tấn công sử dụng khung nội tuyến để phân phối khai thác đến người dùng. Công cụ khai thác chính xác được phân phối và phát hiện bởi một trong những xác nhận này có thể thay đổi thường xuyên.

  Hai biến thể IframeRef có mức độ phổ biến cao đã được phân loại lại là biến thể JS/Seedabutor trong 1Q13, nhưng tỷ lệ phát hiện cho IframeRef vẫn cao trong quý đó sau khi các xác nhận phát hiện cho biến thể Trojan:JS/IframeRef.K được thêm vào các sản phẩm chống phần mềm độc hại của Microsoft nhằm đối phó lại các cuộc tấn công được gọi là "Darkleech", có khả năng thêm các khung nội tuyến độc hại vào các trang web được lưu trên máy chủ web Apache bị xâm phạm.

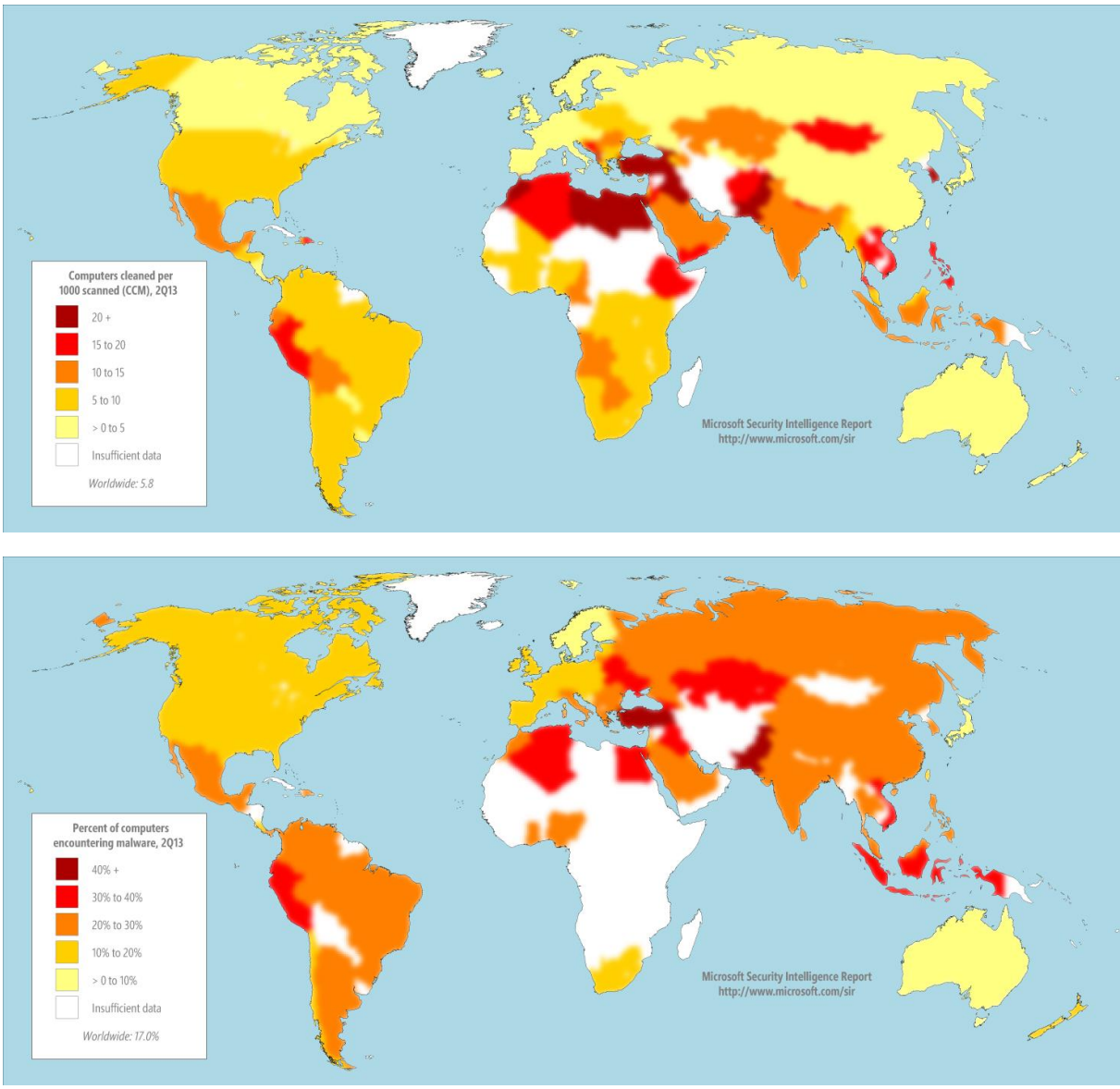
Phần mềm độc hại

Thông tin trong phần này được tổng hợp từ dữ liệu đo lường từ xa được tạo ra từ nhiều nguồn, bao gồm trên một tỷ máy tính trên toàn thế giới và một số dịch vụ bận rộn nhất trên Internet.

Tập này của *Báo cáo Điều tra An ninh mạng của Microsoft* bao gồm một cơ chế mới để đo lường mức độ phổ biến của phần mềm độc hại được gọi là *tỷ lệ phát hiện*. Một số biểu đồ trong phần này, cùng với phân tích kèm theo, biểu thị dữ liệu tỷ lệ phát hiện cùng với dữ liệu tỷ lệ nhiễm, được đo bằng hệ thống đo lường CCM đã được xây dựng.

Đối với quan điểm về mô hình mối đe dọa trên toàn thế giới, Hình 5 cho thấy tỷ lệ nhiễm và tỷ lệ phát hiện tại các địa điểm trên thế giới trong quý hai năm 2013.

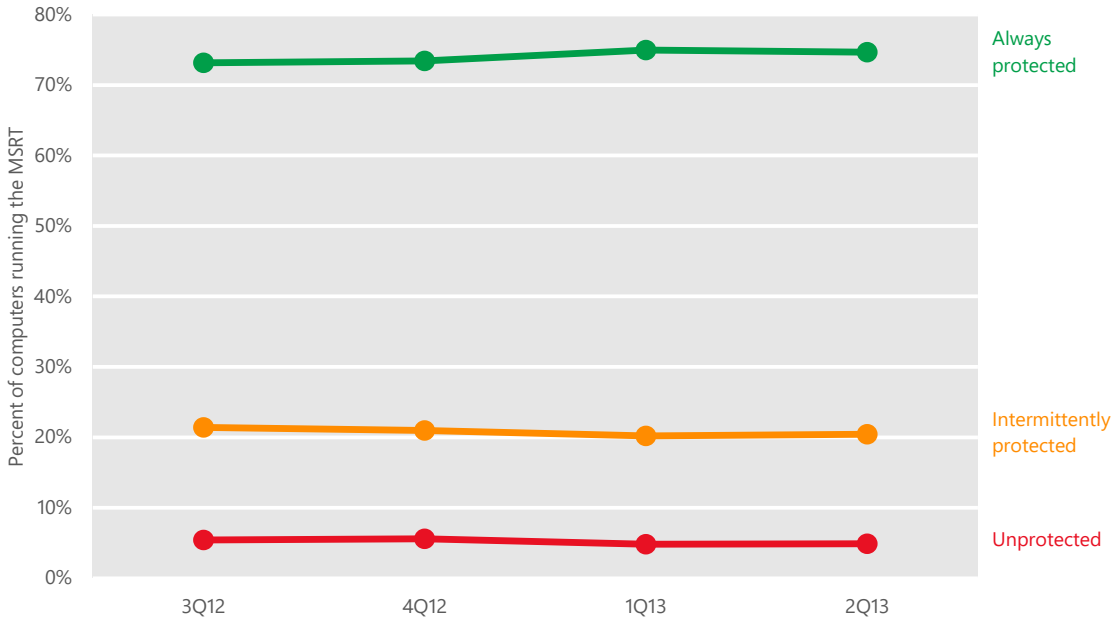
Hình 5. Tỷ lệ nhiễm (trên) và tỷ lệ phát hiện (dưới) theo quốc gia/vùng trong 2Q13



Sử dụng phần mềm bảo mật

Các bản phát hành gần đây của MSRT thu thập và báo cáo chi tiết về trạng thái của phần mềm chống phần mềm độc hại thời gian thực trên máy tính, nếu quản trị viên máy tính đã chọn tham gia cung cấp dữ liệu cho Microsoft. Phương pháp đo lường từ xa này giúp chúng tôi có thể phân tích mô hình sử dụng phần mềm bảo mật trên toàn thế giới và đối chiếu với tỷ lệ nhiễm. Hình 6 biểu thị tỷ lệ phần trăm các máy tính trên toàn thế giới mà MSRT thấy rằng được bảo vệ hoặc không được bảo vệ bằng phần mềm bảo mật thời gian thực trong mỗi quý từ 3Q12 đến 2Q13.

Hình 6. Tỷ lệ phần trăm các máy tính trên thế giới được bảo vệ bằng phần mềm bảo mật thời gian thực, 3Q12–2Q13

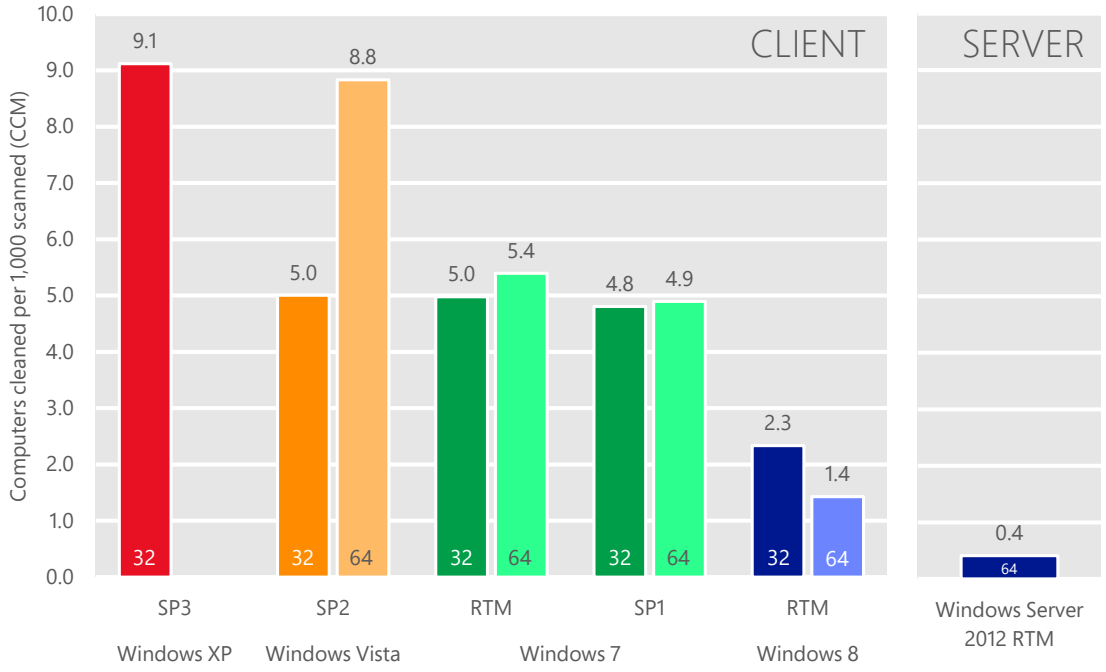


Tỷ lệ nhiễm và tỷ lệ phát hiện theo hệ điều hành

Các tính năng và cập nhật có sẵn với các phiên bản hệ điều hành Windows khác nhau và sự khác biệt trong cách mọi người và tổ chức sử dụng từng

phiên bản ảnh hưởng đến tỷ lệ nhiễm cho các phiên bản và gói dịch vụ khác nhau. Hình 7 biểu thị tỷ lệ nhiễm cho từng kết hợp hệ điều hành Windows/gói dịch vụ đang được hỗ trợ chiếm tối thiểu 0,1% trong tổng số các lần thực thi MSRT trong 2Q13.

Hình 7. Tỷ lệ nhiễm (CCM) theo hệ điều hành và gói dịch vụ trong 2Q13

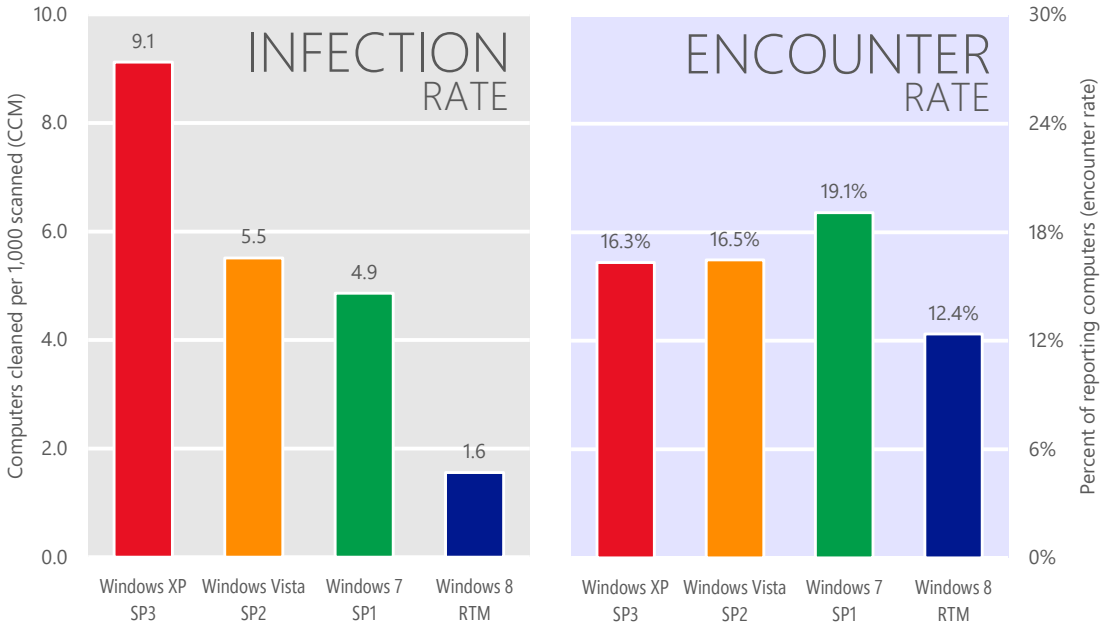


"32" = phiên bản 32-bit; "64" = phiên bản 64-bit. SP = Gói Dịch vụ. RTM = phát hành để sản suất. Các hệ điều hành chiếm tối thiểu 0,1% trong tổng số các lần thực thi MSRT trong 2Q13.

- Dữ liệu này được chuẩn hóa; nghĩa là, tỷ lệ nhiễm cho từng phiên bản Windows được tính bằng cách so sánh số lượng máy tính bằng nhau cho từng phiên bản (ví dụ: 1.000 máy tính Windows XP SP3 với 1.000 máy tính Windows 8 RTM).

Hình 8 biểu thị sự chênh lệch giữa tỷ lệ nhiễm và tỷ lệ phát hiện cho các hệ điều hành máy khách Windows được hỗ trợ trong 2Q13 (gộp chung cả phiên bản 32-bit và 64-bit).

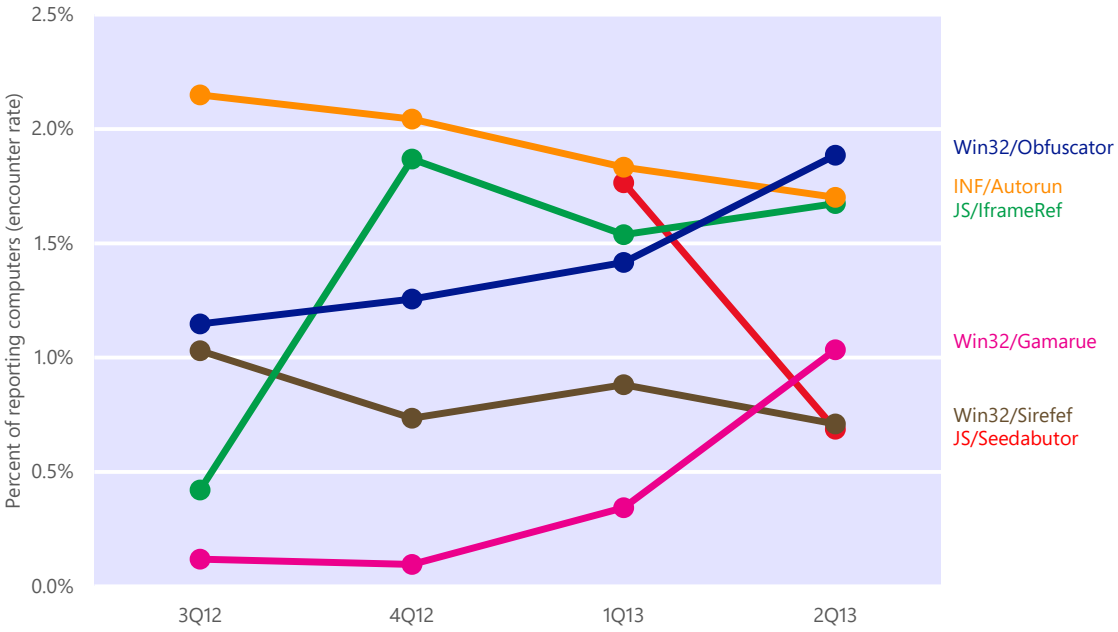
Hình 8. Tỷ lệ nhiễm và tỷ lệ phát hiện cho các hệ điều hành máy khách Windows, 2Q13



Các dòng mối đe dọa

Hình 9 biểu thị xu hướng phát hiện cho một số dòng tăng hoặc giảm đáng kể trong bốn quý vừa qua.

Hình 9. Xu hướng phát hiện cho một số dòng phần mềm độc hại đáng chú ý, 3Q12–2Q13

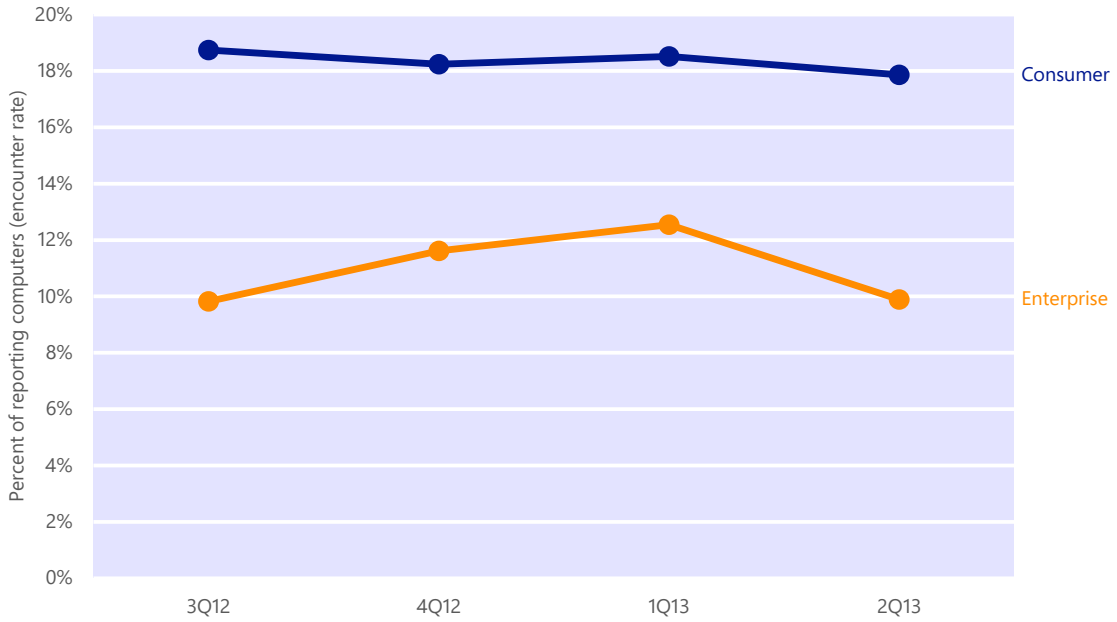

2.5%
2.0%
1.5%
1.0%
0.5%
0.0%
Percent of reporting computers (encounter rate)
3Q12
4Q12
1Q13
2Q13
Win32/Obfuscator
INF/Autorun
JS/IframeRef
Win32/Gamarue
Win32/Sirefef
JS/Seedabutor

- Các phát hiện chung Win32/Obfuscator, INF/Autorun, và HTML/IframeRef là các mối đe dọa phát hiện phổ biến nhất trong 1H13. Autorun, mối đe dọa phát hiện phổ biến nhất trên thế giới trong khoảng thời gian này, là một phát hiện chung cho các loại sâu lây lan giữa các ổ đĩa được gắn bằng tính năng AutoRun của Windows. Sự thay đổi tính năng trong Windows XP và Windows Vista đã làm giảm hiệu quả của kỹ thuật này theo thời gian, nhưng những kẻ tấn công vẫn tiếp tục phát tán phần mềm độc hại nhắm tới tính năng này và các sản phẩm chống phần mềm độc hai của Microsoft đã phát hiện và ngăn chặn những nỗ lực đó ngay cả khi những nỗ lực đó sẽ không thành công.
- Số lần phát hiện Obfuscator đã tăng từ vị trí thứ tư trong 1Q13 lên vị trí thứ nhất trong 2Q13, khiến đây trở thành mối đe dọa phát hiện phổ biến thứ hai trên thế giới trong cả nửa năm. Obfuscator là sự phát hiện chung đối với các chương trình đã bị các công cụ rắc rối hóa độc hại sửa đổi. Những công cụ này thường sử dụng kết hợp các phương pháp, bao gồm mã hóa, nén và chống gỡ lỗi hoặc kỹ thuật chống mô phỏng, để sửa đổi chương trình độc hại nhằm cản trở việc phân tích hoặc phát hiện của các sản phẩm bảo mật. Kết quả thường là một chương trình khác vẫn có chức năng như chương trình gốc nhưng có mã, dữ liệu và hình thái khác.

Mối đe dọa cho cá nhân và doanh nghiệp

Mô hình sử dụng của người dùng cá nhân và người dùng doanh nghiệp có xu hướng rất khác biệt. Việc phân tích những khác biệt này có thể cung cấp chi tiết về những cách thức khác nhau mà kẻ tấn công nhắm tới người dùng doanh nghiệp và cá nhân, cũng như mối đe dọa nào có khả năng thành công trong từng môi trường.

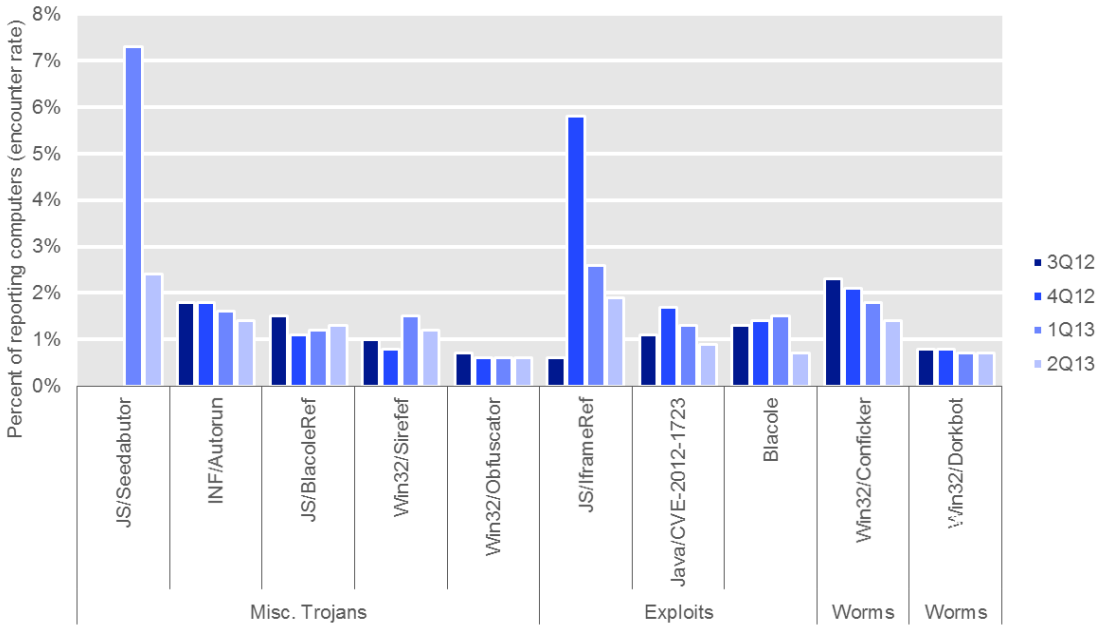
Hình 10. Tỷ lệ phát hiện phần mềm độc hại cho máy tính tiêu dùng và doanh nghiệp, 3Q12–2Q13



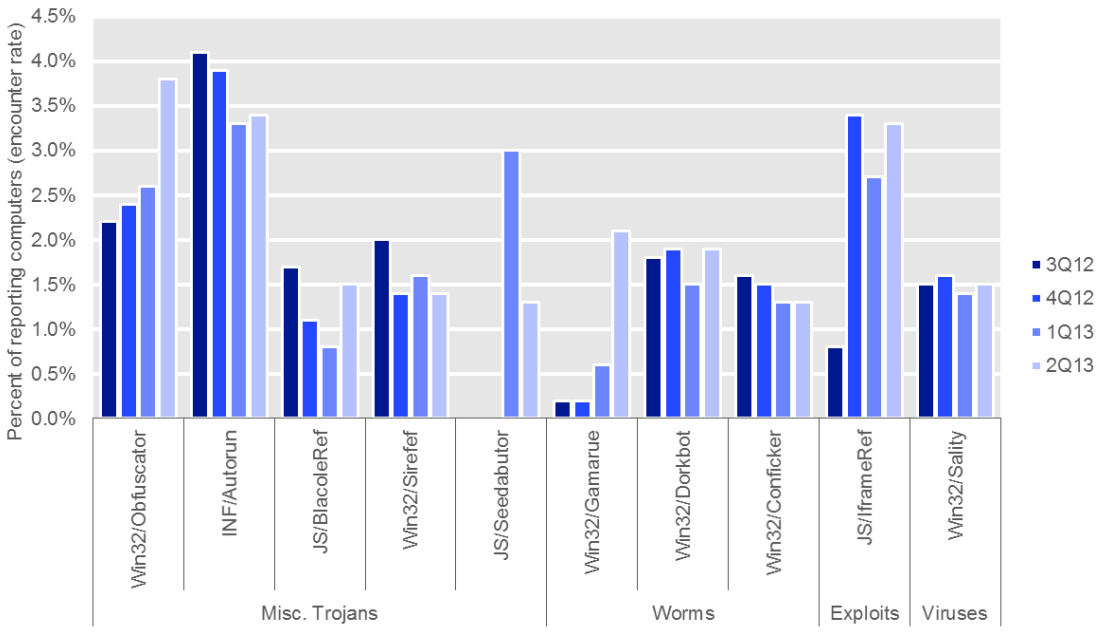
- Môi trường doanh nghiệp thường triển khai các biện pháp bảo vệ chuyên sâu, như tường lửa doanh nghiệp ngăn chặn số lượng phần mềm độc hại nhất định trong việc tiếp cận máy tính của người dùng. Do đó, các máy tính doanh nghiệp có xu hướng phát hiện phần mềm độc hại ở tỷ lệ thấp hơn so với máy tính tiêu dùng. Tỷ lệ phát hiện cho các máy tính tiêu dùng cao gấp 1,5 lần so với các máy tính doanh nghiệp trong 1Q13, với sự chênh lệch tương đối tăng lên 1,8 lần trong 2Q13.

Hình 11 và Hình 12 lần lượt liệt kê 10 dòng hàng đầu được phát hiện bởi các sản phẩm bảo mật doanh nghiệp và tiêu dùng trong 1H13.

Hình 11. Xu hướng hàng quý cho 10 dòng hàng đầu được các sản phẩm bảo mật doanh nghiệp của Microsoft phát hiện trong 1H13, theo tỷ lệ phần trăm máy tính phát hiện mỗi dòng



Hình 12. Xu hướng hàng quý cho 10 dòng hàng đầu được các sản phẩm bảo mật tiêu dùng của Microsoft phát hiện trong 1H13, theo tỷ lệ phần trăm máy tính phát hiện mỗi dòng



- Tám dòng chung cho cả hai danh sách. Trong số này, chỉ Win32/Conficker và JS/Seedabutor phổ biến hơn trên máy tính tiêu dùng so với máy tính doanh nghiệp. Hai dòng khai thác, Java/CVE-2012-1723 và Blacole, nằm trong nhóm 10 mối đe dọa hàng đầu cho doanh nghiệp nhưng không có trong danh sách cho tiêu dùng. Dòng sâu Win32/Gamarue và dòng vi-rút Win32/Sality nằm trong nhóm 10 mối đe dọa hàng đầu cho máy tính tiêu dùng nhưng không có trong danh sách cho doanh nghiệp.
- Các phát hiện chung Win32/Obfuscator và INF/Autorun, mối đe dọa phát hiện phổ biến nhất và thứ hai trên máy tính tiêu dùng, ít gặp hơn trên máy tính doanh nghiệp. Số lần phát hiện Obfuscator trên máy tính doanh nghiệp trong 2Q13 (tỷ lệ phát hiện bằng 3,8%) cao gấp trên sáu lần so với máy tính tiêu dùng (tỷ lệ phát hiện bằng 0,6%). Số lần phát hiện Autorun trên máy tính

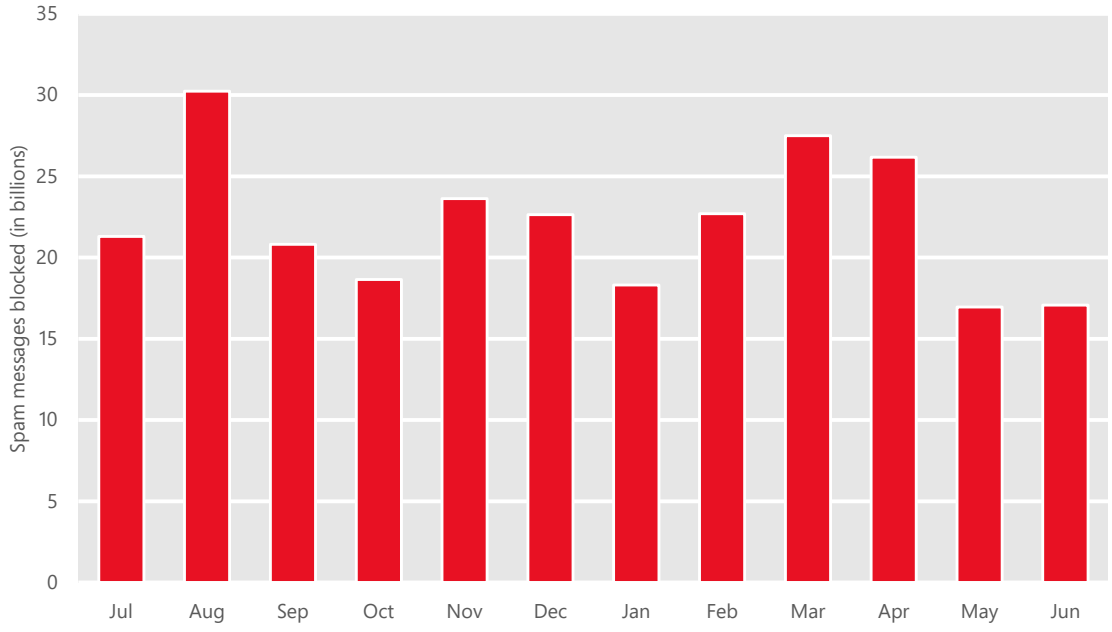
doanh nghiệp (tỷ lệ phát hiện bằng 3,4%) cao gấp trên hai lần so với máy tính tiêu dùng (tỷ lệ phát hiện bằng 1,4%).

Mối đe dọa từ email

Thư rác bị chặn

Thông tin trong phần này của *Báo cáo Điều tra An ninh mạng của Microsoft* được tập hợp từ dữ liệu đo lường từ xa từ Exchange Online Protection, cung cấp các dịch vụ lọc thư rác, lừa đảo và phần mềm độc hại cho hàng chục nghìn khách hàng doanh nghiệp của Microsoft, gửi và nhận hàng chục tỷ thư mỗi tháng.

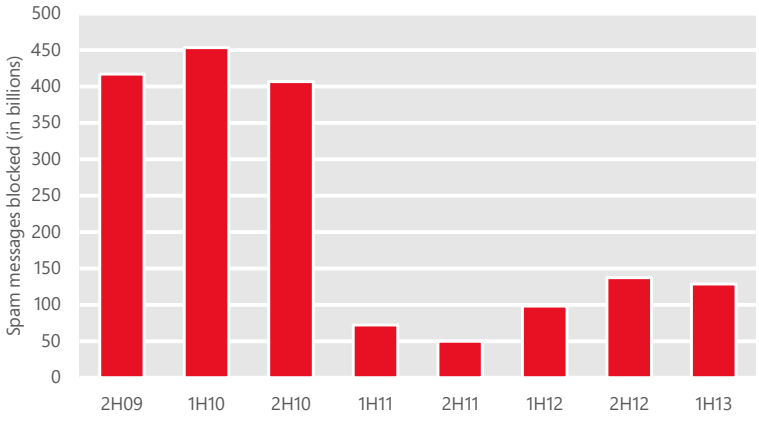
Hình 13. Thư bị chặn bởi Exchange Online Protection, Tháng 7 năm 2012–Tháng 6 năm 2013



- Lượng thư bị chặn trong 1H13 tăng nhẹ so với 2H12, nhưng vẫn ở mức rất thấp so với cuối năm 2010. Sự giảm xuống đáng kể về lượng thư rác phát hiện được từ năm 2010 đã diễn ra trong quá trình loại bỏ thành công một số lượng lớn các botnet gửi thư rác lớn, đáng chú ý là Cutwail (Tháng 8 năm

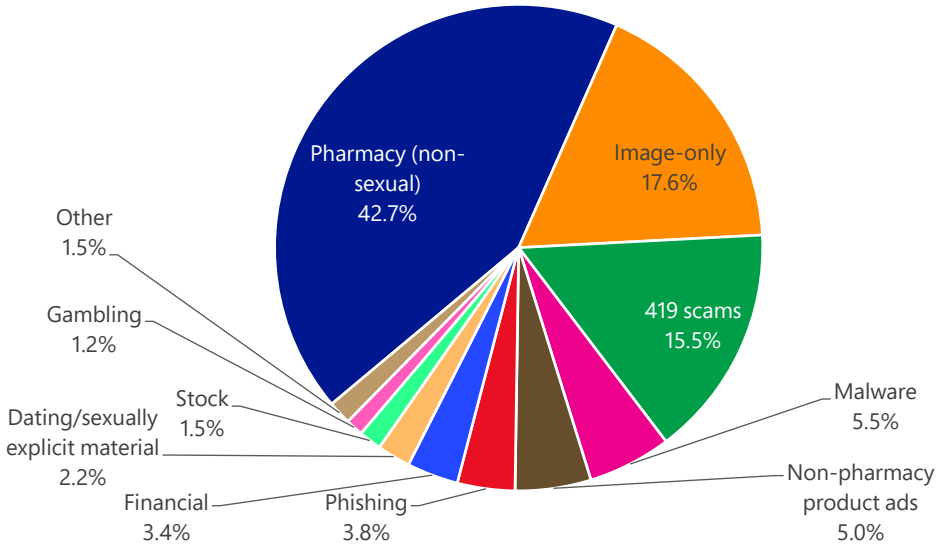
2010) và Rustock (Tháng 3 năm 2011).[2] Trong 1H13, Exchange Online Protection đã xác định rằng có khoảng 1/4 các email không yêu cầu chặn hoặc lọc, so với chỉ 1/33 thư trong năm 2010.

Hình 14. Thư bị chặn bởi Exchange Online Protection trong khoảng thời gian nửa năm, 2H09–1H13



[2] Để biết thêm thông tin về việc xóa bỏ Cutwail, hãy xem *Báo cáo Thông tin Bảo mật của Microsoft, Tập 10 (Tháng 7-Tháng 12, 2010)*. Để biết thêm thông tin về việc xóa bỏ Rustock, hãy xem "Battling the Rustock Threat", có trong Trung tâm Tải về của Microsoft.

Hình 15. Thư đến bị chặn bởi bộ lọc Exchange Online Protection trong 1H13, theo danh mục



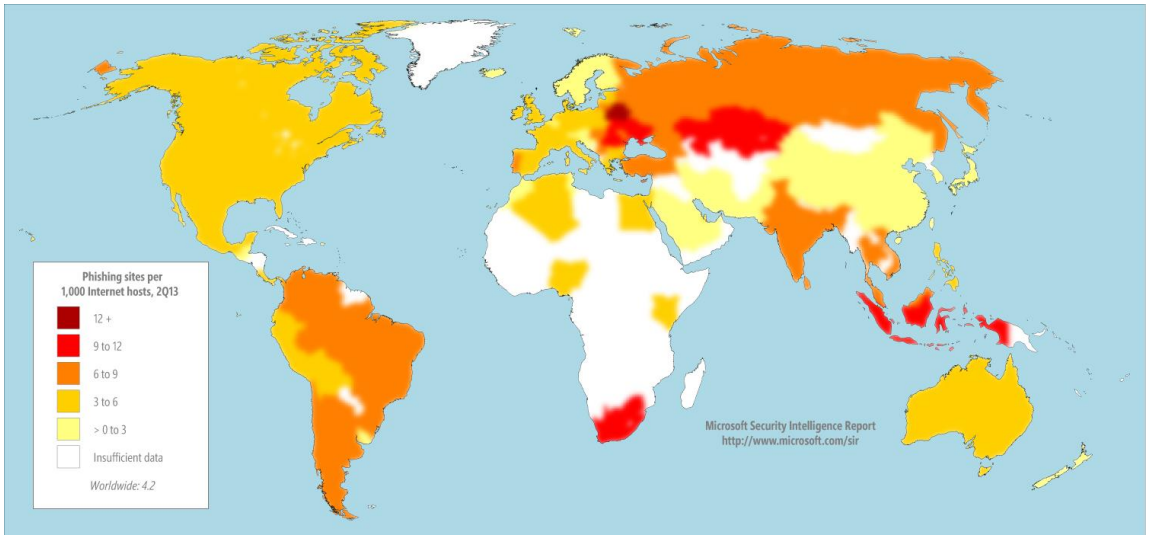
- Các bộ lọc nội dung của Exchange Online Protection nhận diện một số loại thư rác phổ biến khác nhau. Hình 15 biểu thị mức độ phổ biến tương đối của các loại thư rác đã phát hiện trong 1H13.

Trang web độc hại

Trang web lừa đảo

Các trang web lừa đảo được lưu trữ trên khắp thế giới trên các trang lưu trữ miễn phí, trên máy chủ web bị xâm phạm và trong rất nhiều bối cảnh khác.

Hình 16. Số lượng trang web lừa đảo trên 1.000 máy chủ Internet tại các địa điểm trên thế giới trong 2Q13

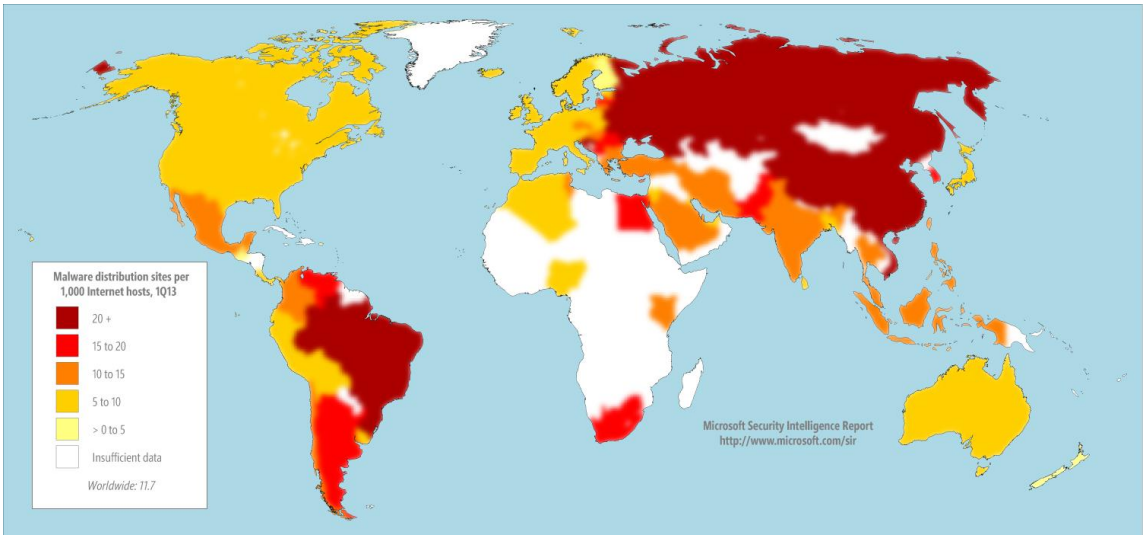


- SmartScreen Filter đã phát hiện 4,2 trang web lừa đảo trên 1.000 máy chủ Internet trên toàn thế giới trong 2Q13.
- Các địa điểm với mật độ trang web lừa đảo trên trung bình bao gồm (11,6 trên 1.000 máy chủ Internet trong 2Q13), Ukraina (10,9) và Nga (8,5). Các địa điểm có mật độ trang web lừa đảo thấp bao gồm Đài Loan (1,2), Nhật Bản (1,3), và Hàn Quốc (1,9).

Trang web lưu trữ phần mềm độc hại

SmartScreen Filter trong Internet Explorer giúp bảo vệ chống lại các trang web đã biết chứa phần mềm độc hại, cùng với trang web lừa đảo. SmartScreen Filter sử dụng các tệp và dữ liệu danh tiếng URL và công nghệ chống phần mềm độc hại của Microsoft để xác định xem trang web có phân phối nội dung không an toàn không. Đối với trang web lừa đảo, Microsoft thu thập dữ liệu ẩn danh liên quan đến số lượng người truy cập từng trang web lưu trữ phần mềm độc hại và sử dụng thông tin này để cải thiện SmartScreen Filter nhằm đối phó tốt hơn với việc phân phối phần mềm độc hại.

Hình 17. Trang web phân phối phần mềm độc hại trên 1.000 máy chủ Internet cho các địa điểm trên thế giới trong 2Q13



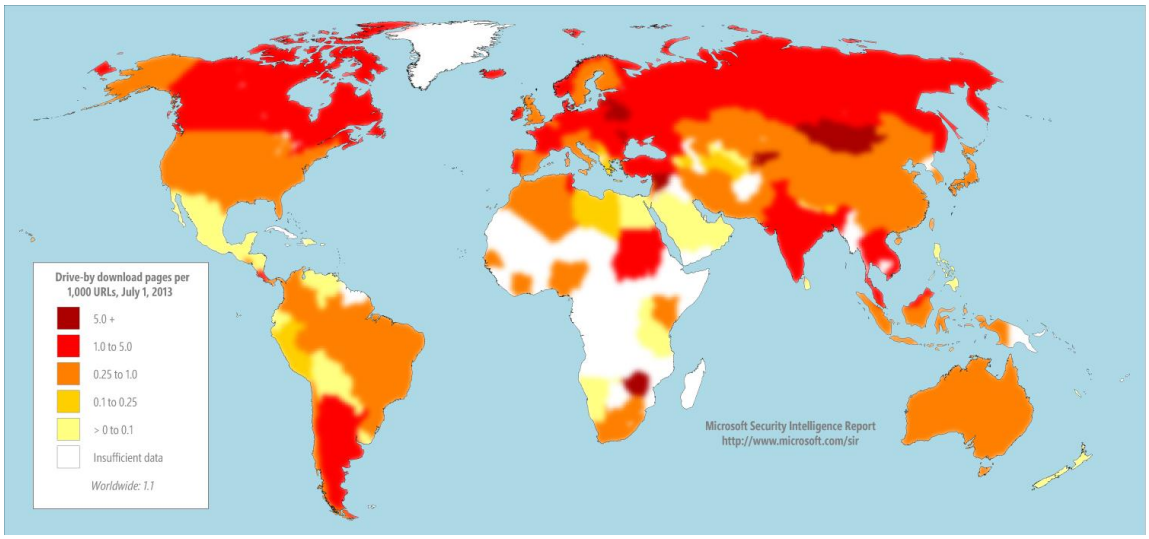
- Các trang web lưu trữ phần mềm độc hại phổ biến hơn rất nhiều so với trang web lừa đảo trong 1H13. SmartScreen Filter đã phát hiện 11,7 trang web lưu trữ phần mềm độc hại trên 1000 máy chủ Internet trên toàn thế giới trong 1Q13, và 17,7 trên 1000 máy chủ trong 2Q13.
- Trung Quốc, có mật độ trang web lừa đảo dưới trung bình (2,3 trang web lừa đảo trên 1000 máy chủ Internet trong 2Q13), cũng có mật độ trang web lưu trữ phần mềm độc hại cao (37,7 trang web lưu trữ phần mềm độc hại

trên 1000 máy chủ trong 2Q13). Các địa điểm khác có mật độ trang web lưu trữ phần mềm độc hại cao bao gồm Ukraina (71,2), Nga (43,6), và Brazil (33,6). Các địa điểm có mật độ trang web lưu trữ phần mềm độc hại thấp bao gồm Phần Lan (6,1), Đan Mạch (7,0), và Nhật Bản (7,0).

Trang web tải về tự động

Trang web *tải về tự động* là trang web lưu trữ một hoặc nhiều công cụ khai thác nhắm đến các lỗ hổng trong trình duyệt web và tiện ích bổ sung của trình duyệt. Người dùng có máy tính dễ bị tấn công có thể bị nhiễm phần mềm độc hại dễ dàng bằng cách truy cập trang web, ngay cả khi không cố gắng tải về bất kỳ thứ gì.

Hình 18. Các trang tải về tự động do Bing lập chỉ mục vào cuối 2Q13 (dưới), trên 1000 URL tại mỗi quốc gia/vùng



Tài liệu này phân tích các điểm chính của báo cáo. Trang web *SIR* cũng cung cấp phân tích chuyên sâu về các xu hướng được phát hiện tại trên 100 quốc gia/vùng trên thế giới và đưa ra các gợi ý nhằm giúp quản lý rủi ro đối với tổ chức, phần mềm và nhân viên của bạn.

Bạn có thể tải *SIRv15* về từ www.microsoft.com/sir.

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security