UNODC
Cơ quan Phòng chống Ma túy và Tội phạm của Liên Hợp Quốc

Mối đe dọa của Tội phạm mạng Darknet đối với Đông Nam Á

2020

CYBERCRIME

Tuyên bố từ chối trách nhiệm

Báo cáo này chưa được chỉnh sửa chính thức.

Nội dung của ấn phẩm này không nhất thiết phản ánh quan điểm hoặc chính sách của UNODC, các Quốc gia Thành viên, hoặc các tổ chức đóng góp và chúng cũng không ngụ ý bất kỳ sự chứng thực nào.

Các ký hiệu được sử dụng và việc trình bày tài liệu trong ấn phẩm này không ngụ ý việc thể hiện bất kỳ quan điểm nào của UNODC hoặc Ban Thư ký Liên Hợp Quốc liên quan đến tình trạng pháp lý của bất kỳ quốc gia, vùng lãnh thổ, thành phố hoặc khu vực nào hoặc của các cơ quan chức năng của họ, hoặc liên quan đến việc phân định biên giới hoặc ranh giới của họ.

Lời nói đầu

Cơ quan Phòng chống Ma túy và Tội phạm của Liên Hợp Quốc (UNODC) tự hào giới thiệu bản phân tích giới thiệu này về các mối đe dọa có liên quan đến darknet đối với các quốc gia Đông Nam Á, được thực hiện thông qua mối quan hệ đối tác mạnh mẽ với các cơ quan hành pháp và tư pháp toàn cầu và khu vực, cùng với ngành tư nhân và giới học viện. Báo cáo được thực hiện nhờ sự tài trợ tự nguyện của Chính phủ Nhật Bản.

Báo cáo này đánh giá Darkweb từ góc độ người dùng, tội phạm và cơ quan thực thi pháp luật, đặc biệt tập trung vào tội phạm mạng nhắm vào các quốc gia Đông Nam Á. Darknet (như các mạng trên Darkweb) cung cấp môi trường lý tưởng cho một loạt các hoạt động tội phạm. Giống như các mối đe dọa mới xuất hiện trên Clearnet (như mạng Internet thông thường), darknet có thể tạo điều kiện cho các cuộc tấn công tương tự mang lại cho thủ phạm khả năng ẩn danh cao hơn. Khả năng ẩn danh này khiến cho việc điều tra và ngăn chặn trở nên khó khăn hơn, nhưng vẫn có thể thực hiện được.

Đã có sự gia tăng đồng đều trong việc sử dụng darknet và Darkweb, cả vì lý do hợp pháp và bất hợp pháp, trong khi đại dịch COVID-19 dường như cũng làm phát sinh tội phạm mạng darknet, bao gồm cả những tội phạm không có kinh nghiệm phạm tội trên mạng trước đó. Mặc dù vậy, có rất ít dữ liệu về tội phạm darknet cụ thể cho khu vực Đông Nam Á. Có rất ít ưu tiên cho tội phạm darknet trong khu vực, cả về chính sách lẫn thực tiễn. Điều này tạo ra rủi ro từ chính hành vi phạm tội, kết hợp với phản ứng hạn chế về chính trị, chính sách và của cơ quan thực thi pháp luật. Cần phải có lãnh đạo cấp bộ trưởng về các vấn đề mạng ở mỗi quốc gia để đảm bảo rằng những người thực thi pháp luật nhận được sự hỗ trợ về chính trị cần thiết để thực hiện các hoạt động khó khăn nhất.

Có thể dự đoán và ngăn chặn nhiều hoạt động phạm tội diễn ra trên darknet. UNODC và các đối tác luôn nỗ lực để giải quyết những thách thức này bằng cách hỗ trợ và khuyến khích phát triển chính sách, hỗ trợ nghiên cứu, hỗ trợ đào tạo và nâng cao năng lực ở Đông Nam Á.

Nhận thức là cơ sở để giải quyết vấn đề tội phạm mạng. Tuy nhiên, trước những thách thức do darknet đặt ra, các bên liên quan phải tăng cường cam kết và hợp tác để xây dựng chính sách, chia sẻ thông tin tình báo và tăng cường hợp tác quốc tế để chống lại tội phạm darknet trong nước, khu vực và quốc tế.

Phân tích này của UNODC sẽ cung cấp thông tin cho các nhà hoạch định chính sách ở Đông Nam Á, bao gồm thông qua Hội nghị Quan chức Cấp cao về Tội phạm Xuyên quốc gia (SOMTC) hàng năm, cũng như hỗ trợ các cơ quan thực thi pháp luật và hợp tác tư pháp, đồng thời tạo cơ hội cho việc phòng chống tội phạm tập trung vào darknet.

Jeremy Douglas
Đại diện Khu vực,
Đông Nam Á và Thái Bình Dương

Neil J. Walsh
Trưởng Bộ phận Tội phạm mạng và
Chống rửa tiền

Mục lục

Lời cảm ơn

UNODC xin cảm ơn Chính phủ các nước Đông Nam Á – Brunei Darussalam, Campuchia, Indonesia, Cộng hòa Dân chủ Nhân dân Lào, Malaysia, Myanmar, Philippines, Singapore, Thái Lan và Việt Nam đã hỗ trợ trong quá trình lập báo cáo này. Việc chuẩn bị báo cáo này sẽ không thể hoàn thành nếu không có sự hỗ trợ của họ.

UNODC chân thành cảm ơn sự đóng góp tài chính của Chính phủ Nhật Bản để thực hiện nghiên cứu này.

Nghiên cứu này được Chương trình Toàn cầu về Tội phạm Mạng của UNODC thực hiện thông thành viên khu vực có trụ sở tại Văn phòng Khu vực Đông Nam Á và Thái Bình Dương (ROSEAP).

Giám sát

Jeremy Douglas, Đại diện Khu vực, Đông Nam Á và Thái Bình Dương.
Neil J. Walsh, Trưởng Bộ phận Tội phạm mạng và Chống rửa tiền.

Đội ngũ nòng cốt

Alexandru Caciuloiu (điều phối, phân tích, xem xét và soạn thảo)
Pawinee (Ann) Parnitudom (thu thập dữ liệu)
Mikko Niemelae, Joshua James (phân tích và soạn thảo)
Juha Nurmi (nghiên cứu và dữ liệu)
Praphaphorn Tamarpirat (hỗ trợ hành chính và hậu cần)

Báo cáo này cũng có sự đóng góp từ các nguồn thông tin có giá trị của nhiều nhân viên UNODC và các chuyên gia và tổ chức bên ngoài, những người đã xem xét hoặc đóng góp vào các phần khác nhau của báo cáo, bao gồm Live Brenna, Kamola Ibragimova và Himal Ojha.

Các từ viết tắt

APT	Tấn công có chủ đích
ASEAN	Hiệp hội các Quốc gia Đông Nam Á
ATM	Máy rút tiền Tự động
CaaS	Tội phạm/Tội phạm mạng như một Dịch vụ
CAPTCHA	Phép thử Tự động để Phân biệt Máy tính và Con người
CSE	Bóc lột Tình dục Trẻ em
CSEM	Tài liệu về Bóc lột Tình dục Trẻ em
DoS	Từ chối Dịch vụ
DDoS	Từ chối Dịch vụ Phân tán
FATF	Lực lượng Đặc nhiệm Tài chính Quốc tế
IP	Giao thức Internet
IRC	Chat Chuyển tiếp Internet
MaaS	Phần mềm độc hại như một Dịch vụ
NCMEC	Trung tâm Quốc gia về Trẻ em Mất tích và Bị bóc lột
OCSE	Bóc lột Tình dục Trẻ em Trực tuyến
PGP	Pretty Good Privacy (Bảo mật rất mạnh)
PoS	Điểm Bán hàng
RaaS	Mã độc tống tiền như một Dịch vụ
SOMTC	Hội nghị Quan chức Cấp cao về Tội phạm Xuyên quốc gia
Tor	Trình duyệt Tor
UNODC	Cơ quan Phòng chống Ma túy và Tội phạm của Liên Hợp Quốc
12P	Dự án Internet Vô hình

Giá Phạm tội
trên Darkweb

DDOS Tấn công **từ** **$50** một gnày

Lấy cắp dữ liệu trang web **từ** **$490**

Lấy cắp dữ liệu trang web **từ** **$150**

Đánh cắp số thẻ tín dụng **từ** **$9**

Phần mềm độc hại ăn cắp mật khẩu **từ** **$150**

Đánh cắp dữ liệu thanh toán **từ** **$270**

Lấy cắp email **từ** **$40**

Tấn công có mục tiêu **từ** **$490**

Nguồn: Positive Technologies https://www.ptsecurity.com/ww-en/analytics/darkweb-2018/

Bản tóm tắt

Mọi người từ tất cả các quốc gia Đông Nam Á đều sử dụng darknet, phổ biến nhất là The Onion Router, thường được gọi là Trình duyệt Tor. Mặc dù có thể đưa ra ước tính sơ bộ về số lượng người dùng darknet trong một quốc gia, nhưng việc xác định chính xác lý do họ sử dụng darknet lại không khả thi. Các yếu tố thúc đẩy nổi bật dường như là biện pháp bảo vệ quyền riêng tư và tránh né sự kiểm duyệt trực tuyến bên cạnh những yếu tố do những kẻ phạm tội trên mạng sử dụng. Việc sử dụng darknet và Darkweb cho hành vi phạm tội trên mạng (như tất cả nội dung được lưu trữ trên darknet) khác nhau. Đối với một số người, đây là đòn bẩy để bắt đầu các cuộc tấn công mạng, đối với những người khác, đây là nơi để truy cập các sản phẩm và dịch vụ bất hợp pháp, trong khi đối với những người khác, đây là nơi cung cấp quyền riêng tư và ẩn danh hợp pháp từ các doanh nghiệp đang theo dõi và sử dụng dữ liệu cá nhân của họ.

Có rất ít bằng chứng cho thấy việc chống lại tội phạm mạng sử dụng darknet là một chính sách hoặc ưu tiên hoạt động trong khu vực. Do đó, nhìn chung là thiếu dữ liệu nhất quán, định lượng và định tính để có thể rút ra các phân tích. Điều này dẫn đến một chu kỳ tồn tại lâu dài về các lỗ hổng chính sách, hạn chế khả năng nhận biết mối đe dọa, ưu tiên và huy động nguồn lực của cơ quan thực thi pháp luật. Đáng quan tâm hơn, điều này sẽ tạo ra cơ hội cho hành vi bóc lột tội phạm mà nạn nhân không có quyền truy đòi.

Mạng Tor là darknet lớn nhất và có hầu hết các trang web. Giữa năm 2020, có khoảng 200.000 dịch vụ onion trên toàn thế giới (các máy chủ bên trong darknet Tor). Cũng giống như các máy chủ trên Clearnet, một số máy chủ này lưu trữ các trang web, trong khi những máy chủ khác lưu trữ các dịch vụ email hoặc chia sẻ tệp. Một số trong số đó được sử dụng cho mục đích phạm tội. Đồng thời, tiền điện tử và các ứng dụng liên lạc ẩn danh đã thúc đẩy việc sử dụng cả darknet và Darkweb nói chung, đồng thời góp phần vào hoạt động buôn bán các sản phẩm và dịch vụ bất hợp pháp.

Hành vi vi phạm dữ liệu ảnh hưởng đến thông tin cá nhân của các cá nhân, doanh nghiệp và tổ chức đã tăng đáng kể trong hai năm qua. Dữ liệu thường bị bán hoặc bị rò rỉ trên các trang web Darkweb, nơi thúc đẩy hàng loạt các cuộc tấn công mạng và tội phạm mạng. Dữ liệu bị rò rỉ này thường dẫn đến các cuộc tấn công nhắm vào một nạn nhân cụ thể, lừa đảo, lập hóa đơn giả, đánh cắp thẻ tín dụng, mạo danh và bán tài liệu mật. Số lượng marketplace trong mạng Tor đã tăng từ một vào năm 2011 lên 118 vào năm 2019. Cũng đã có sự gia tăng lớn về số lượng và sự đa dạng của các sản phẩm để bán. Ví dụ: số lượng sản phẩm độc quyền có trên Darkweb marketplace phổ biến, Valhalla, đã tăng từ 5.000 vào năm 2015 lên 13.000 vào năm 2018. Các sản phẩm có sẵn bao gồm ma túy (bao gồm cocaine, heroin và opioid), súng ống và đạn dược, các công cụ và dịch vụ xâm nhập và nhiều loại sản phẩm khác. Một số marketplace cũng chuyên buôn bán thông tin thẻ thanh toán và tài liệu giả mạo.

Báo cáo Ma túy Thế giới năm 2019 của UNODC[1] ước tính rằng số người mua ma túy qua Darkweb đã tăng gấp đôi từ 4,7% vào tháng 1 năm 2014 lên 10,7% vào tháng 1 năm 2019. Hoạt động mua ma túy qua Darkweb vẫn là một hiện tượng mới nổi với gần một nửa số người cho biết đã mua ma túy qua Darkweb vào năm 2019 cho biết họ chỉ mới bắt đầu sử dụng phương thức mua hàng này trong hai năm qua. Tuy nhiên, nhìn chung, tác động của Darkweb đối với vấn đề ma túy trên thế giới hiện đang ở mức thấp.

Ví dụ, giao diện người dùng ngày càng trở nên thân thiện với nhà cung cấp, cho phép đặt hàng số lượng lớn và kết hợp các đơn đặt hàng của các sản phẩm khác nhau vào một lần vận chuyển. Các nhà cung cấp cũng nhận thức rõ hơn về khả năng gỡ bỏ các marketplace của cơ quan quản lý, họ sẽ chống lại bằng cách hoạt động đồng thời trên nhiều thị trường.

Từ năm 2015 đến 2019, số lượng tài liệu bóc lột tình dục trẻ em (CSEM) trên Tor đã tăng từ 170 trang web CSEM độc quyền lên 776 trang web.[2] Tài liệu lạm dụng mới được đăng liên tục, trong khi nội dung đã công bố trước đó được đăng lại thường xuyên. Điều này khiến việc cung cấp các số liệu đáng tin cậy về quy mô chính xác của mối đe dọa trở nên khó

khăn và đặc biệt gây khó khăn cho cơ quan thực thi pháp luật trong việc tìm kiếm và phân loại các mối đe dọa ưu tiên.Những rủi ro gây ra cho trẻ em và hoạt động của cơ quan thực thi pháp luật từ Darkweb là rất lớn. Những kẻ lạm dụng liên tục thảo luận về cách gây tổn hại cho các cuộc điều tra của cơ quan thực thi pháp luật, cách giảm thiểu nguy cơ bị phát hiện và cách tiếp cận các nạn nhân trẻ em mới để bóc lột và lạm dụng.

Darkweb thu hút các trang web CSEM vì nó cung cấp tính năng ẩn danh, cũng như hoạt động kiểm duyệt trực tuyến linh hoạt. Rất khó để gỡ bỏ loại nội dung bất hợp pháp này vì nhiều trang CSEM sao chép nội dung của họ ở những nơi khác.

Tháng 11 năm 2019, số lượng trang web CSEM chiếm 5% tổng số trang web Darkweb[3] nhưng thời gian đóng cửa do đại dịch COVID-19 có thể đã làm tăng quy mô của các trang web đó. Hơn nữa, số lượng tài liệu về hành vi lạm dụng (chủ yếu là hình ảnh và video) hiện có, thể hiện số lượng đáng kể dữ liệu tổng thể được chia sẻ trên Darkweb, với một số trang web cho rằng họ đã tích lũy được vài terabyte tài liệu về hành vi lạm dụng (tương đương với giá trị của 80 ngày video hoặc gần 1 triệu ảnh kỹ thuật số).

Nhìn chung, khối lượng nội dung trên darknet và lượng người sử dụng chúng (đặc biệt là Tor) đang tăng liên tục. Mặc dù không phải tất cả các hoạt động trên darknet đều bất hợp pháp, nhưng chắc chắn rằng những tên tội phạm có tổ chức hoạt động trong Darkweb đang không ngừng phát triển khả năng, cơ chế bảo mật và phương thức kinh doanh của chúng.

Các chính phủ ở Đông Nam Á cần bắt đầu đầu tư các nguồn lực cần thiết để phân tích và chống lại tội phạm mạng sử dụng Tor đồng thời nâng cao khả năng hoạt động trên các darknet khác nhau. Đồng thời, cần điều chỉnh cẩn thận biện pháp ứng phó để đảm bảo bảo vệ quyền con người và quyền riêng tư hợp pháp.

Khi các darknet tăng cường mức độ bảo mật của mình, việc có được quyền truy cập và có tác động có ý nghĩa trở nên phức tạp và tốn kém hơn, khiến việc đạt được tiến bộ ở cấp quốc gia ngày càng khó khăn. Thay vào đó, việc phối hợp cùng nhau trên phạm vi quốc tế và sử dụng các chuyên gia được đào tạo chuyên sâu được trang bị các kỹ năng và công nghệ mới nhất đã được chứng minh là một giải pháp hiệu quả hơn.

Đông Nam Á và Darkweb

Do bản chất của darknet và Darkweb, không dễ để liên kết bất kỳ hành động phạm tội cụ thể nào với người dùng ở Đông Nam Á – vị trí phạm tội thường chỉ được xác định rõ ràng ngay trước thời điểm kẻ phạm tội bị bắt. Tuy nhiên, có bằng chứng rõ ràng về các nạn nhân Đông Nam Á trên Darkweb. Điều quan trọng là các nước Đông Nam Á phải mở rộng quy mô chính sách, hoạt động thực thi pháp luật và năng lực tư pháp của họ để chống lại tội phạm darknet.

Những phát hiện chính

CÓ RẤT ÍT DỮ LIỆU ĐÁNG TIN CẬY VỀ TỘI PHẠM SỬ DỤNG DARKNET Ở ĐÔNG NAM Á

Có rất ít bằng chứng cho thấy việc chống lại tội phạm mạng sử dụng darknet là một chính sách hoặc ưu tiên hoạt động trong khu vực. Do đó, nhìn chung là thiếu dữ liệu nhất quán, định lượng và định tính để có thể rút ra các phân tích. Điều này dẫn đến một chu kỳ tồn tại lâu dài về các lỗ hổng chính sách, hạn chế khả năng nhận biết mối đe dọa, ưu tiên và huy động nguồn lực của cơ quan thực thi pháp luật. Đáng quan tâm hơn, điều này sẽ tạo ra cơ hội cho hành vi bóc lột tội phạm mà nạn nhân không có quyền truy đòi.

TỘI PHẠM MẠNG DARKNET ĐƯỢC CHO LÀ ĐANG GIA TĂNG TẠI ĐÔNG NAM Á

Ngày càng nhiều tội phạm ở Đông Nam Á có khả năng sử dụng Tor darknet để tham gia vào vố số các hoạt động bất hợp pháp có sẵn trên Darkweb. Trong đó bao gồm hoạt động mua và bán ma túy, bộ công cụ tội phạm mạng, hộ chiếu giả, tiền tệ giả, tài liệu bóc lột tình dục trẻ em trực tuyến, đánh cắp thông tin chi tiết thẻ tín dụng và thông tin nhận dạng cá nhân do hành vi vi phạm.

NGÔN NGỮ VÀ PHƯƠNG NGỮ CỦA ĐÔNG NAM Á TRÊN DARKWEB THAY ĐỔI THEO THỜI GIAN

Tiếng Anh là ngôn ngữ sử dụng chính cho tội phạm mạng trên Darkweb, mặc dù nội dung có nguồn gốc địa phương bằng các ngôn ngữ của Đông Nam Á đang trở nên phổ biến. Do đó, có một cơ sở khách hàng. Và mặc dù điều này cho thấy một mối đe dọa về tội phạm mạng đa dạng, nhưng nó cũng tạo ra cơ hội cho các hoạt động xâm nhập và ngăn chặn tương xứng, hợp pháp, có trách nhiệm và cần thiết của cơ quan thực thi pháp luật đòi hỏi phải có các khuôn khổ lập pháp và giám sát nhân quyền rõ ràng và mạnh mẽ.

TIỀN ĐIỆN TỬ LÀ PHƯƠNG THỨC THANH TOÁN ĐƯỢC CHỌN

Tiền điện tử là phương thức thanh toán hàng đầu trên darknet.Tiền điện tử và các dịch vụ rửa tiền có liên quan đang phát triển khi những kẻ tội phạm tìm cách hướng tới các loại tiền tệ đảm bảo tính riêng tư hơn. Bitcoin vẫn là công cụ chính để trao đổi tiền điện tử sang tiền pháp định (tiền tệ do một quốc gia phát hành). Điều này cho thấy các cơ hội về chính sách, lập pháp và điều tra. Các quốc gia được khuyến khích tham gia cùng UNODC, Lực lượng Đặc nhiệm Tài chính Quốc tế (FATF) và ngành công nghiệp để chống lại mối đe dọa do các dòng tài chính bất hợp pháp sử dụng tài sản ảo và hoạt động rửa tiền gây ra.

HẦU HẾT CÁC HOẠT ĐỘNG THỰC THI PHÁP LUẬT TRÊN DARKWEB ĐỀU BẮT NGUỒN TỪ QUỐC TẾ. NĂNG LỰC TRONG NƯỚC CÓ GIỚI HẠN

Mặc dù đã có các hoạt động thực thi pháp luật nhắm vào tội phạm mạng darknet ở Đông Nam Á, nhưng các hoạt động này là kết quả của các cuộc điều tra quốc tế được thực hiện bên ngoài khu vực, chỉ có một số lượng nhỏ các trường hợp bắt nguồn từ chính khu vực. Tội phạm mạng có thể sẽ coi Đông Nam Á là một môi trường hoạt động có rủi ro tương đối thấp/thu lợi cao vì khả năng bị phát hiện tương đối thấp. Các chiến dịch phòng chống có thể có tác động.

Kiến nghị

CÁC QUỐC GIA NÊN TĂNG CƯỜNG CHÍNH SÁCH DARKNET CHUYÊN BIỆT VÀ NĂNG LỰC HOẠT ĐỘNG

Mỗi quốc gia Đông Nam Á phải tăng cường hiểu biết về chính trị, chính sách và hoạt động chuyên môn liên quan đến mạng darknet, các dịch vụ, các cuộc điều tra về tiền điện tử và thu thập thông tin tình báo. Điều này sẽ tăng cường vấn đề an ninh quốc gia, hợp tác quốc tế và xây dựng lòng tin trong ngoại giao không gian mạng phòng ngừa.

CẦN PHẢI CÓ MỘT BAN LÃNH ĐẠO CẤP BỘ HOẶC ĐẠI SỨ VỀ CÁC VẤN ĐỀ MẠNG ĐƯỢC HỖ TRỢ BẰNG NĂNG THỰC THI PHÁP LUẬT CÓ CHUYÊN MÔN

Các hoạt động thực thi pháp luật trên darknet cần có các cán bộ được đào tạo và có chuyên môn cao. Những cán bộ này phải có hiểu biết sâu rộng về pháp luật, Internet, nhân quyền, quyền riêng tư, công nghệ truyền thông, tiền điện tử, kỹ thuật mã hóa và ẩn danh, bao gồm cả các kỹ năng điều tra chuyên môn. Ngoài khả năng chiến lược, cần có ban lãnh đạo cấp Bộ hoặc Đại sứ về vấn đề mạng đối với tất cả các vấn đề mạng. Điều này đảm bảo tính nhất quán trong chính sách giữa các chính phủ và cơ chế cần thiết để các nhà thực thi pháp luật tìm kiếm các biện pháp giám sát, thử thách hoặc hỗ trợ về mặt chính trị đối với các phương pháp điều hành mới.

CÁC QUỐC GIA NÊN NGĂN CHẶN VIỆC GIAO NHẬN BƯU KIỆN BẤT HỢP PHÁP CÓ LIÊN QUAN VÀ TIẾN HÀNH MỘT BIỆN PHÁP TIẾP CẬN PHƯƠNG TIỆN TRUYỀN THÔNG CHỦ ĐỘNG

Thị trường Darknet tạo điều kiện cho hoạt động bán hàng hóa thực, như ma túy và vũ khí. Tăng cường năng lực trong nước và hợp tác quốc tế để phát hiện các bưu kiện bất hợp pháp sẽ ngăn chặn việc lưu thông các hàng hóa bất hợp pháp, cũng như làm suy giảm uy tín của những người bán hàng trên thị trường về mặt tâm lý.

ÁP DỤNG CÁC CHÍNH SÁCH VÀ QUY ĐỊNH VỀ TIỀN ĐIỆN TỬ (TÀI SẢN ẢO)

Quy định về người dùng và sàn giao dịch tiền điện tử, đặc biệt là sử dụng các nguyên tắc tiếp cận dựa trên rủi ro tài sản ảo của FATF, sẽ hỗ trợ đáng kể trong việc giảm thiểu hoạt động chuyển tiền ẩn danh.

TẠO RA CHIẾN LƯỢC CHỐNG TỘI PHẠM MẠNG DARKNET TRONG KHU VỰC

Cần tạo ra một kế hoạch và một chiến lược khu vực để hợp tác và ứng phó cùng với Hội nghị Quan chức Cấp cao về Tội phạm Xuyên quốc gia (SOMTC) của ASEAN và các bên liên quan khác.

TIẾP TỤC NGHIÊN CỨU

Nâng cao năng lực trong nước trong các ngành công, tư và học thuật để khuyến khích tiếp tục nghiên cứu về các công nghệ, chính sách và kỹ thuật điều tra về darknet tương xứng, hợp pháp, có trách nhiệm và cần thiết trong khuôn khổ Nhân quyền rộng lớn.

Giới thiệu

Tội phạm mạng là một dạng tội phạm xuyên quốc gia đang phát triển.Tính chất phức tạp của tội phạm, vì hành vi phạm tội diễn ra trong phạm vi không gian mạng không biên giới (nơi thủ phạm và nạn nhân có thể ở các khu vực khác nhau), cùng với sự tham gia ngày càng nhiều của các nhóm tội phạm có tổ chức. Ảnh hưởng của tội phạm mạng có thể lan truyền khắp các xã hội trên toàn thế giới, đặt ra nhu cầu cần phải có một biện pháp ứng phó khẩn cấp, năng động và mang tính quốc tế.

Ngày càng có nhiều tội phạm sử dụng darknet để che dấu các hoạt động của chúng. Khi nội dung và dịch vụ bất hợp pháp được lưu trữ trên Darkweb sẽ khiến cho việc điều tra trở nên phức tạp hơn. Darknet cũng được sử dụng như một cầu nối ẩn danh để thực hiện các cuộc tấn công mạng thông thường.

Tất nhiên, có những cách sử dụng darknet hợp pháp. Nhiều người dùng coi các hoạt động quảng cáo và thu thập dữ liệu tích cực của các tổ chức công và tư là hành vi xâm phạm quyền riêng tư của họ. Trong những trường hợp này, darknet được sử dụng để giảm bớt những lo ngại về quyền riêng tư của những người dùng tuân thủ luật pháp. Do đó, một số trình duyệt web phổ biến hiện đang sử dụng định tuyến darknet (thường là Tor) làm tính năng bảo mật. Darknet cũng đã trở thành một công cụ thuận tiện để bảo vệ quyền riêng tư của cơ quan thực thi pháp luật trong quá trình điều tra trực tuyến.

Giống như Internet, darknet được sử dụng cho cả mục đích tốt và xấu. Sự khác biệt chính giữa Clearnet và Darkweb là sau này sẽ khó xác định được việc kiểm duyệt và quyền hạn.

Báo cáo này nhằm tìm hiểu mối đe dọa của tội phạm mạng sử dụng darknet, và đặc biệt là tác động của nó đến các nước Đông Nam Á.

Mục đích

Mục đích của đánh giá này là để đánh giá các mối đe dọa darknet tồn tại trong bối cảnh tội phạm mạng của các nước Đông Nam Á. Những phát hiện trong đánh giá này sẽ tạo ra các cách để thay đổi chính sách, hành động và khuyến nghị.Quá trình thu thập dữ liệu diễn ra vào năm 2019 và đầu năm 2020.

Phương pháp nghiên cứu

Phân tích này bao gồm một đánh giá ban đầu về các chiến lược, kế hoạch, chính sách, khuôn khổ và chương trình về an ninh mạng tại Đông Nam Á. Một cuộc khảo sát với các đại diện chính phủ cũng đã được thực hiện trong các phiên họp của nhóm làm việc về tội phạm mạng. Phân tích kỹ thuật chi tiết và các ví dụ về diễn đàn tội phạm được bao gồm trong các phụ lục của báo cáo này.

CLEARNET

Mạng Internet truy cập
công khai dễ truy cập
bằng kết nối Internet và
trình duyệt thông thường.
Ví dụ về nội dung:
Google, Facebook, YouTube,
Wikipedia, Netflix.

DEEP WEB

Mạng Internet truy cập
công khai không xác định
đối với các công cụ tìm kiếm,
như các trang web được mã hóa
hoặc không được lập chỉ mục,
cơ sở dữ liệu riêng tư và nội dung
không được liên kết khác.
Ví dụ về nội dung:
Cơ sở dữ liệu học thuật, hồ sơ y tế,
hồ sơ tài chính, tài liệu pháp lý,
thông tin chính phủ, quyền truy cập
thư viện, tài khoản ngân hàng.

DARKWEB

Tập hợp các trang web tồn tại trên darknet.
Không thể truy cập trực tiếp từ Clearnet và
thường cần có phần mềm đặc biệt để
truy cập các trang web đó.Các trang web
sử dụng địa chỉ IP ẩn được lưu trữ trên các
mạng được mã hóa an toàn để tăng tính ẩn danh.
Ví dụ về nội dung:
Các trang web được Tor mã hóa, hệ thống tố giác,
dịch vụ email siêu an toàn, thị trường darknet.

Darknet và Darkweb

Darkweb là một phần của World Wide Web và không thể truy cập bằng các trình duyệt web tiêu chuẩn như Internet Explorer, Firefox, Edge hoặc Chrome. Điều này là do các trang web trên Darkweb hoạt động bên trong các mạng được mã hóa đặc biệt để cung cấp tính năng ẩn danh.

Trên Clearnet (các khu vực có thể truy cập mạng Internet công khai mà không cần bất kỳ phần mềm hỗ trợ nào), có thể xác định và theo dõi người dùng. Mặt khác, Darkweb được thiết kế để ngăn chặn tính năng theo dõi. Có thể truy cập thông qua phần mềm miễn phí, dễ truy cập, kết nối các máy tính qua mạng phân tán (darkneti). Bằng cách định tuyến lưu lượng truy cập giữa các máy tính trên darknet, danh tính của người dùng sẽ bị ẩn.

Sau khi được kết nối với darknet, một thiết bị có thể "giao tiếp" với các thiết bị khác cũng được kết nối với cùng darknet. Các darknet thường lưu trữ nội dung "dành riêng cho darknet" và chính nội dung được lưu trữ này tạo nên cái được gọi là "Darkweb". Giống như Clearnet, Darkweb lưu trữ hàng nghìn trang web – nhưng chỉ có thể truy cập được khi chúng được kết nối với darknet.

Trong hai thập kỷ qua, đã có một số darknet phổ biến hoạt động như các mạng đồng cấp:

- 2000: **Freenet**: một phần mềm lưu trữ dữ liệu để chia sẻ tệp và giao tiếp.
- 2001: **GNUnet**: một phần mềm để chia sẻ tệp.
- 2002: **Tor**: một phần mềm để liên lạc ẩn danh.
- 2003: **WASTE**: một phần mềm để chia sẻ tệp và nhắn tin tức thời.
- 2003: **I2P**: một phần mềm để liên lạc ẩn danh.
- 2004: **Dịch vụ Onion**: Tor đã thực hiện chức năng để công khai các trang web ẩn danh.
- 2006: **RetroShare**: một diễn đàn trò chuyện ẩn danh và phần mềm chia sẻ tệp.
- 2011: Thị trường Darkweb đầu tiên, Silk Road, xuất hiện trong mạng **Tor**.

Các mạng phổ biến nhất cho phép Darkweb công khai là mạng Tor và I2P[4,5,6]. Các mạng nhỏ hơn khác (như Freenet, GNUnet và nhiều mạng khác) có ít người dùng hơn nhiều[7]. Như một dấu hiệu cho biết số lượng mạng darknet, Wikipedia liệt kê 22 mạng chia sẻ tệp ẩn danh[8]. Nội dung phân tích trong đánh giá này tập trung vào mạng Tor vì nó hiện là hệ thống darknet phổ biến nhất tại thời điểm viết báo cáo này. Các mạng ẩn danh khác tạo ra rất ít dữ liệu để phân tích riêng.

Mạng Tor cung cấp tính năng ẩn danh cho người dùng Internet và các dịch vụ trực tuyến."Dịch vụ Onion" là các dịch vụ Internet, như trang web, email và chia sẻ tệp, chỉ được cung cấp thông qua mạng Tor.Mạng Tor che giấu địa chỉ IP thực (và ngầm định là vị trí) của máy chủ[9,10,11].

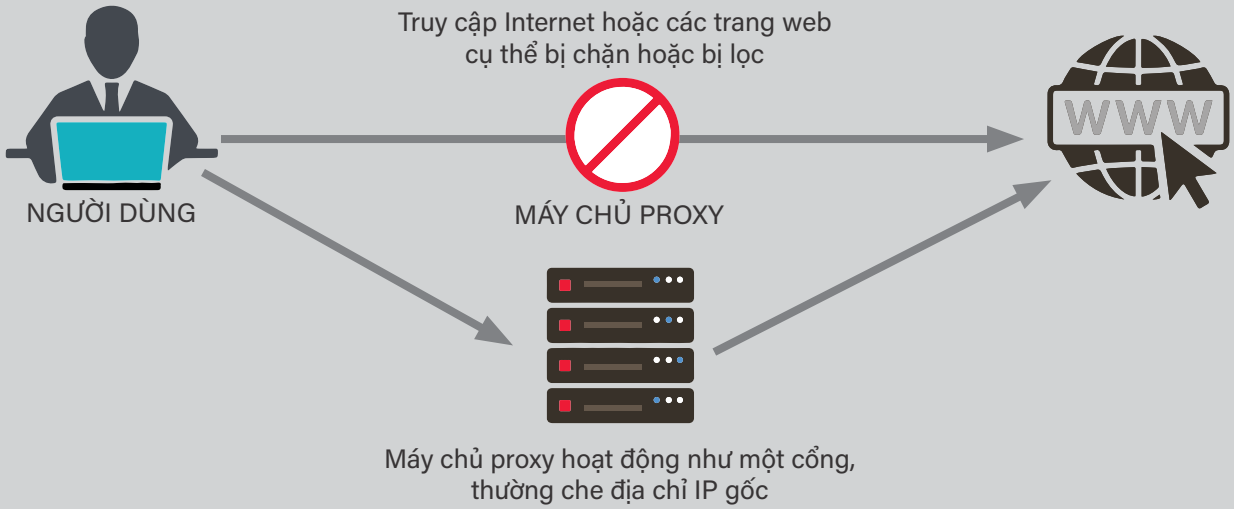
Mạng Tor được bắt đầu sử dụng vào năm 1996 khi thiết kế của Onion Routing được công bố để cung cấp tính năng ẩn danh cho các hệ thống liên lạc[12]. Năm 2004, công tác triển khai kỹ thuật cuối cùng của mạng định tuyến đã được tiến hành. Syverson, Dingledine và Mathewson đã xuất bản bài viết của họ về mạng ***Tor: The Second-Generation Onion Router*** cùng với mã nguồn của Onion Router (Tor)[13]. Kể từ đó, mạng Tor bắt đầu cung cấp tính năng ẩn danh trực tuyến cho các ứng dụng Internet.

Mạng Tor cho phép công bố các dịch vụ Internet ẩn danh. Dịch vụ Onion có địa chỉ Onion (*.onion) và chúng chỉ có thể truy cập được từ bên trong mạng Tor. Ví dụ, https://facebookcorewwwi.onion/ là địa chỉ Onion hợp lệ cho Facebook và có thể được truy cập bằng cách sử dụng Trình duyệt Tor.

Để cho phép trình duyệt web an toàn, ẩn danh, Tor Project đã phát triển Trình duyệt Tor, ứng dụng nhận biết quyền riêng tư chính của họ, có sẵn trên trang web của Tor Project[14]. Trình duyệt Tor dễ sử dụng như một trình duyệt web tiêu chuẩn.Nó đơn giản là một trình duyệt Mozilla Firefox Extended Support Release (ESR) đã được sửa đổi với các tiện ích và cài đặt mặc định được bảo mật tốt nhất.

Tránh kiểm duyệt Internet bằng máy chủ proxy

Tránh kiểm duyệt: biện pháp vượt qua các kỹ thuật kiểm duyệt Internet để truy cập thông tin hoặc dịch vụ bị chặn.

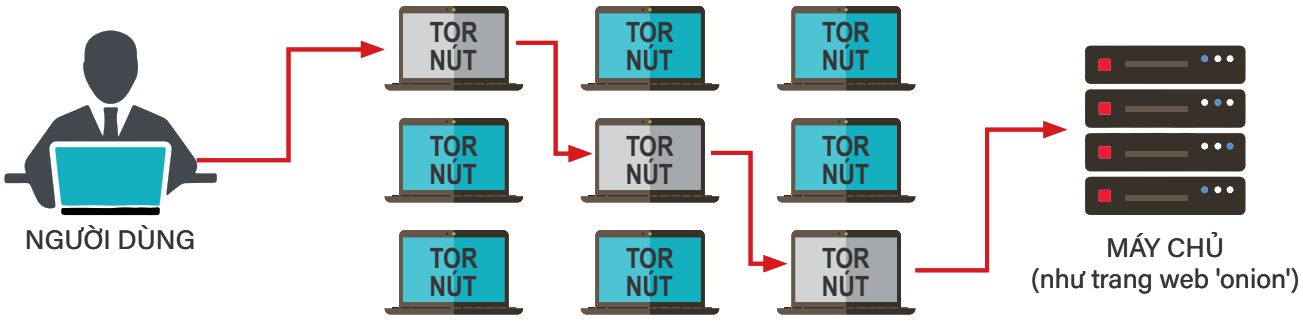


Trình duyệt Tor định tuyến tất cả lưu lượng truy cập web thông qua mạng Tor, loại bỏ hầu hết các phương pháp lấy dấu vân tay (dữ liệu về quyền riêng tư nhạy cảm cục bộ, như lịch sử duyệt web, bộ nhớ cache và cookie) trong quá trình này. Mạng Tor cũng cho phép công bố trang web ẩn danh cho cái gọi là "dịch vụ ẩn" chỉ có thể được truy cập bằng Trình duyệt Tor. Với địa chỉ IP được ẩn, cả người dùng và các trang web công khai đó đã cải thiện tính ẩn danh và, để tránh bị phát hiện thêm, nhiều trang web chỉ trực tuyến trong thời gian ngắn. Điều này khiến cho cả hoạt động thực thi pháp luật chủ động và phản ứng đều trở nên đặc biệt khó khăn.

Số lượng các trang web Onion xác định trên Darkweb đã tăng từ vài trăm vào năm 2012 lên hơn 100.000 vào năm 2020. Trong sáu tháng đầu năm 2020, có 110.865 trang web Onion[15]. Một lý do cho sự tăng trưởng này là do một số trang web phân chia nội dung của họ trên hàng nghìn trang web con, mỗi trang thuộc một miền khác nhau. Đây là một biện pháp phổ biến với các trang web đang chia sẻ tài liệu video, với một số trang web thậm chí còn cung cấp một miền duy nhất cho mỗi video. Lý do cho điều này là để có thể truy cập nội dung nhanh hơn bằng cách sử dụng một số mạch mạng Tor song song. Mỗi miền Onion lại có mạch mạng Tor riêng, đây là nguyên nhân thường gây ra tắc nghẽn lưu lượng. Bằng cách sử dụng nhiều trang web con và tên miền, người dùng có thể tăng tốc độ truy cập bằng cách phân chia nhỏ nội dung. Nó cũng khiến cho việc chặn hợp pháp và thu thập thông tin tình báo kỹ thuật trở nên đặc biệt khó khăn, ngay cả đối với các cơ quan tình báo có năng lực nhất.

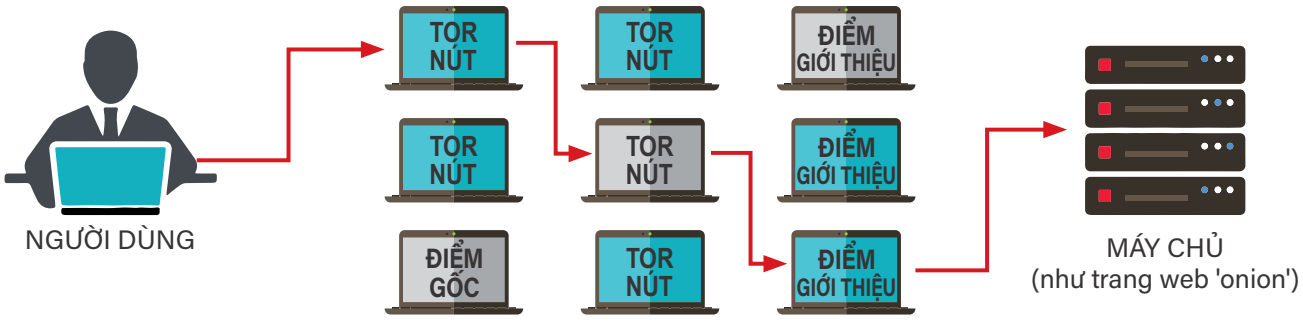
Cách mạng Tor hoạt động

Với trình duyệt Tor, lưu lượng truy cập Internet được định tuyến thông qua một loạt các máy tính tình nguyện khác nhau (được gọi là 'thiết bị chuyển tiếp' hoặc 'nút') và mỗi nút chỉ nhận biết được các nút trước và sau trong mạng. Dữ liệu cũng được mã hóa nhiều lần (giống như các lớp của một củ hành) và định tuyến được chọn ngẫu nhiên và thay đổi liên tục. Điều này đảm bảo rằng địa chỉ IP và vị trí của người dùng ban đầu được ẩn.



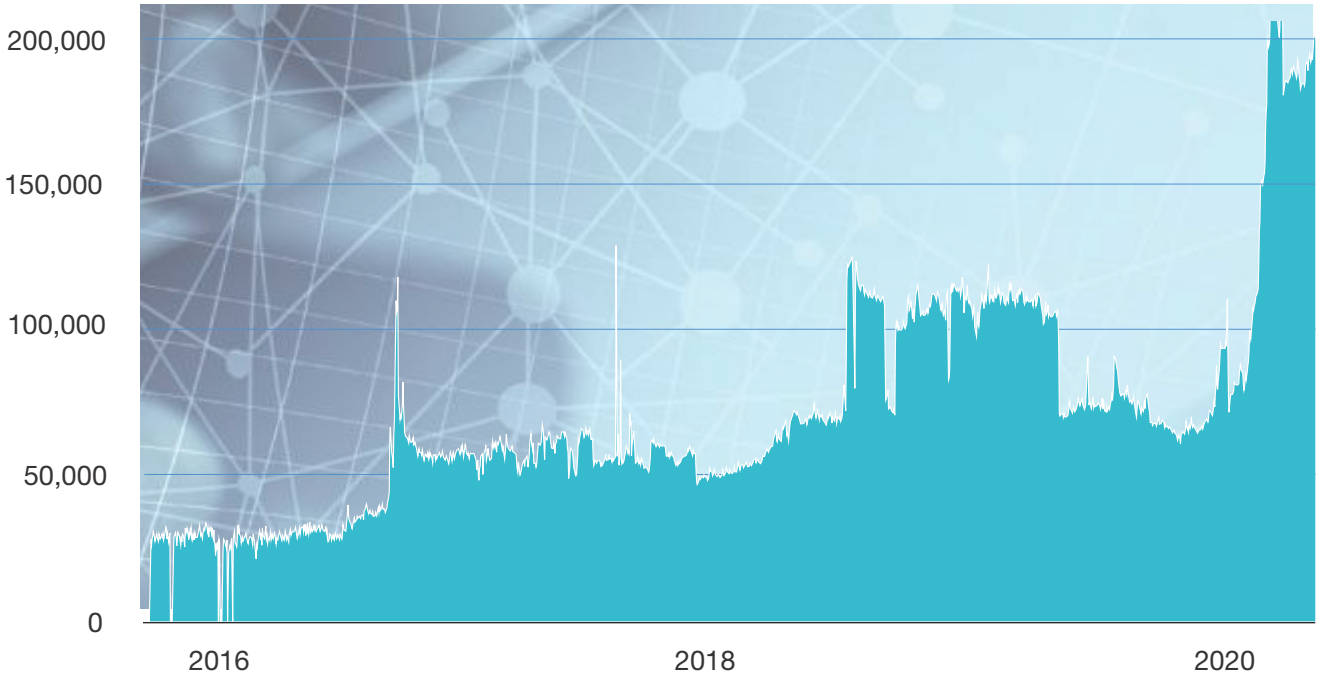
Cách các dịch vụ ẩn của mạng Tor hoạt động

Mạng Tor cũng có thể cung cấp tính năng ẩn danh cho các trang web và các máy chủ khác. Các máy chủ được cấu hình để chỉ nhận các kết nối đến thông qua mạng Tor được gọi là 'dịch vụ ẩn'. Thay vì tiết lộ địa chỉ IP của máy chủ (và vị trí mạng), một dịch vụ ẩn được truy cập thông qua địa chỉ Onion. Mạng Tor có thể định tuyến dữ liệu đến và đi từ các dịch vụ ẩn đồng thời bảo toàn tính ẩn danh của cả hai bên.



Một 'Điểm Giới thiệu' sẽ gửi một thông báo đến máy chủ cho biết có người muốn kết nối.Sau đó, máy chủ sẽ tạo một mạch (thông qua các nút Tor khác) đến một 'Điểm Gốc'. Đường truyền giữa Điểm Giới thiệu và Điểm Gốc được mã hóa từ đầu đến cuối (sử dụng các mã khóa công khai và riêng tư) do đó bảo vệ tính ẩn danh của cả hai bên.

Hình 1. Số lượng trang web có trong mạng Tor.

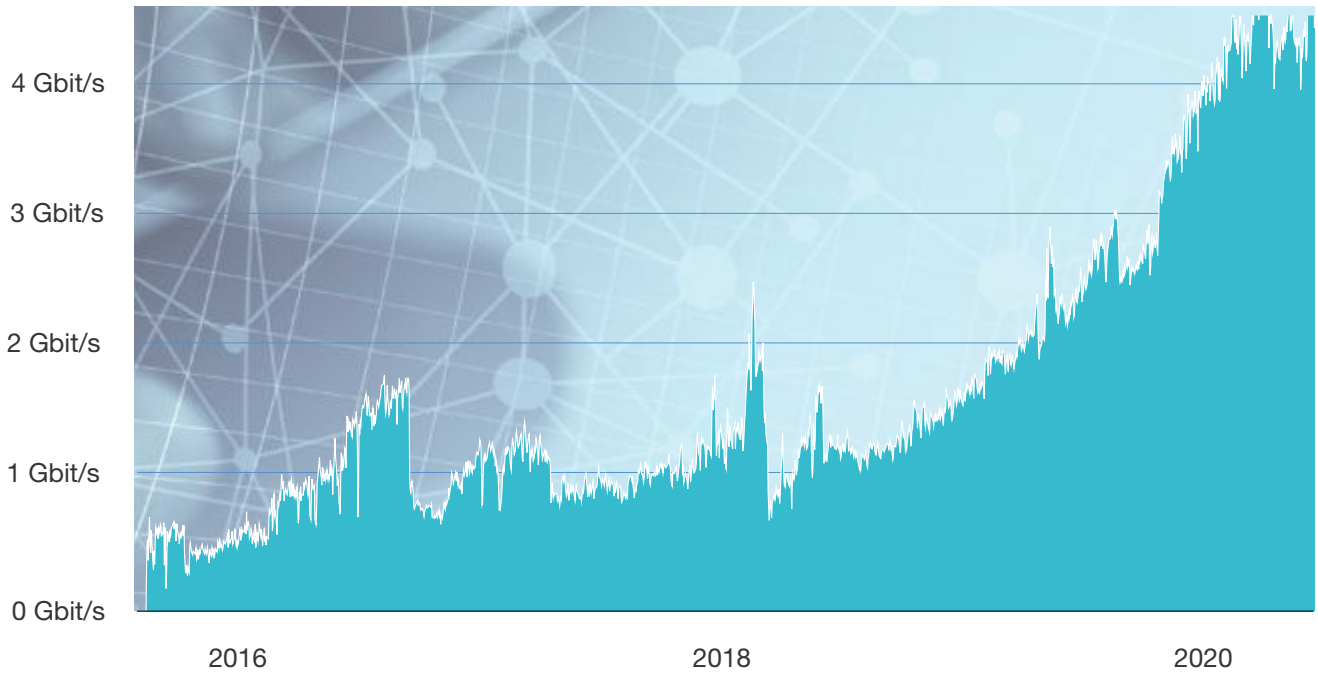


Tor Project - https://metrics.torproject.org/

***Nhiều trang web duy trì trực tuyến chỉ trong khoảng thời gian ngắn. Phép đo chỉ tính toán các trang web có thể truy cập trong thời gian nhất định.**

Lưu lượng truy cập vào các dịch vụ Onion cũng đã tăng lên kể từ năm 2015 và vẫn còn tiếp tục tăng[16]. Điều này có nghĩa là ngày càng có nhiều nội dung được tải lên và tải xuống từ các trang web Onion.

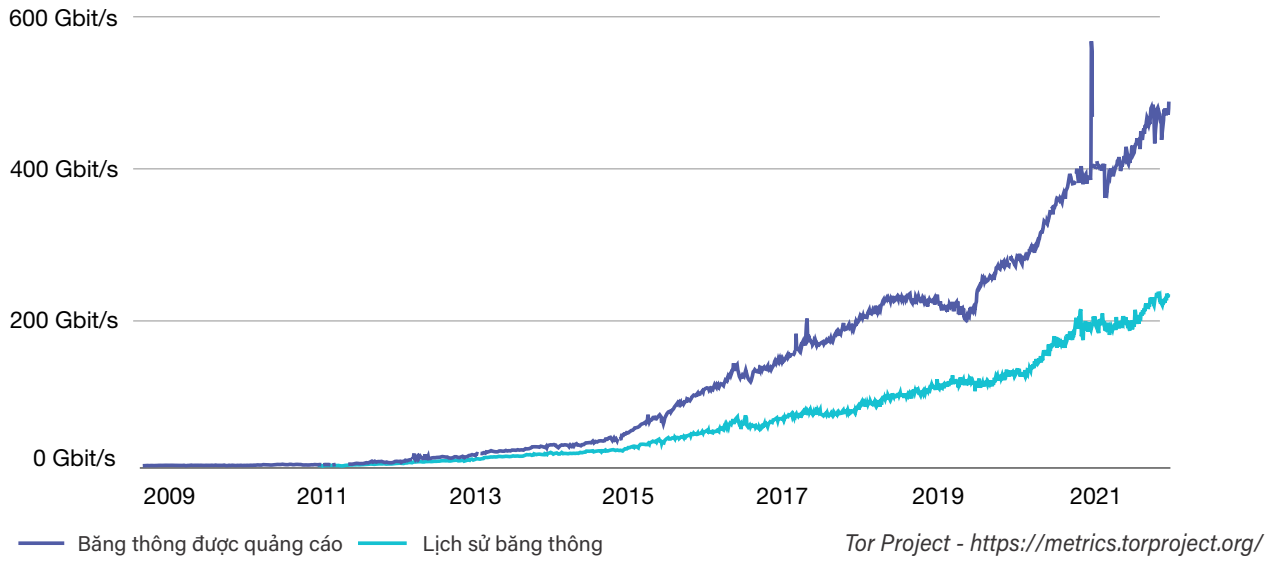
Hình 2. Lưu lượng truy cập vào các dịch vụ Onion (Gbit/s).



Tor Project - https://metrics.torproject.org/

Nhiều người dùng trong mạng Tor tự nguyện cài đặt phần mềm Tor ở "chế độ định tuyến" cho phép máy tính của họ nhận và chuyển lưu lượng truy cập trên mạng Tor. Các máy chủ của máy tính này thường được gọi là bộ định tuyến, thiết bị chuyển tiếp hoặc nút Tor. Năm 2019, có khoảng 7.000 thiết bị chuyển tiếp mạng Tor trên toàn thế giới và 2,5 triệu người dùng Tor[17]. Vì luật chống tội phạm mạng, truy tố và hợp tác quốc tế thường dựa vào quyền tài phán theo khu vực địa lý, rõ ràng là các hoạt động chống tội phạm mạng darknet đặc biệt khó khăn.

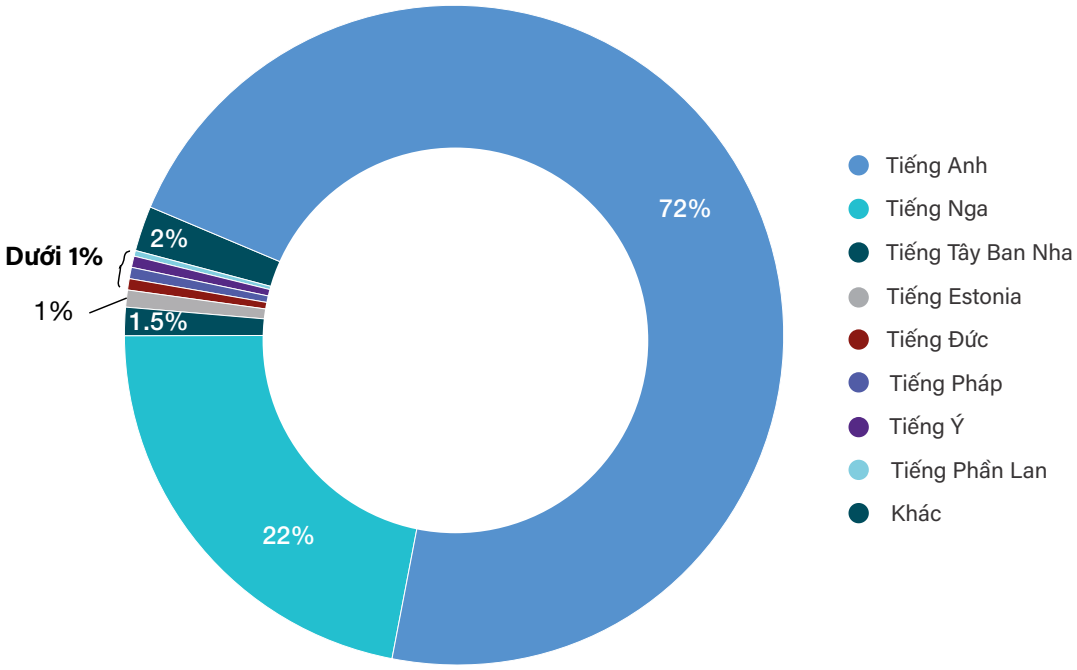
Tổng băng thông mạng Tor là 400 Gbit/s.



Tor Project - https://metrics.torproject.org/

Tổng băng thông của mạng Tor đã tăng đáng kể trong một thập kỷ qua. Năm 2010, lưu lượng truy cập mạng Tor gần như bằng 0 Gbit/s, nhưng con số này đã tăng lên 400 Gbit/s vào năm 2019[18] (tương đương với việc phát trực tuyến 100 bộ phim HD Netflix mỗi giây). Sự gia tăng băng thông này chứng tỏ việc sử dụng mạng Tor đã tăng lên. Trong ***Hình 3***, 'băng thông được quảng cáo' là tổng lượng băng thông có sẵn trong mạng Tor giữa các nút, trong khi 'lịch sử băng thông' là lượng băng thông thực sự được sử dụng trong mạng Tor.

Hình 4. Các ngôn ngữ phổ biến nhất được sử dụng trên mạng Tor vào năm 2019.



Mặc dù nhiều người dùng mạng Tor đã phát triển các cộng đồng bằng tiếng mẹ đẻ của họ, nhưng ngôn ngữ được sử dụng phổ biến nhất là tiếng Anh (khoảng 70%). Một lý do được đưa ra cho việc sử dụng tiếng Anh (ngay cả khi đó không phải là tiếng mẹ đẻ của người dùng) là nó cung cấp thêm một lớp ẩn danh. Quản trị viên của thị trường darknet hoặc các diễn đàn khác trên Darkweb thường sẽ cảnh báo người dùng không sử dụng các ngôn ngữ khác (và không sử dụng tiếng lóng bản địa) làm biện pháp chống giám sát (tiếng địa phương có thể hỗ trợ cơ quan thực thi pháp luật xác định chính xác vị trí hoặc nguồn gốc của người dùng).

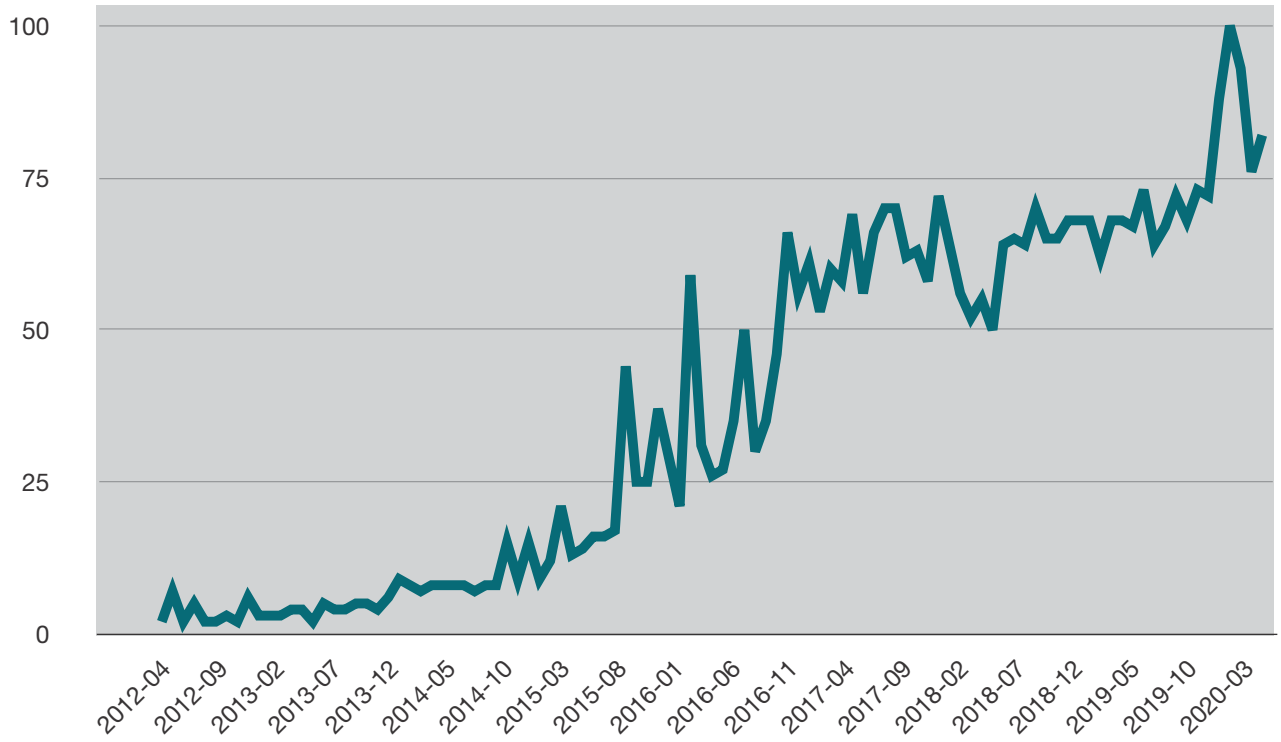
Darkweb và tội phạm mạng

Sự quan tâm của công chúng đến Darkweb đã tăng lên trong những năm qua[19]. Hệ sinh thái ẩn danh đã phát triển từ việc trở thành một kênh giao tiếp cho các tác nhân về quyền riêng tư thành một marketplace toàn cầu với nhiều loại sản phẩm và dịch vụ có sẵn để mua[20]. Darkweb cũng có vai trò là một nền tảng cho một số lượng lớn các diễn đàn thảo luận về nhiều chủ đề. Các diễn đàn này đôi khi được tổ chức theo quốc tịch và ngôn ngữ hoặc theo các loại tội phạm cụ thể như tội phạm thẻ tín dụng, giao dịch nội gián, buôn bán ma túy, buôn bán vũ khí, Tội phạm như một Dịch vụ (CaaS) và chống hoặc chống lại sự giám sát của các nhà điều tra trực tuyến[21].

Khi bọn tội phạm sử dụng Darkweb ngày càng nhiều, nó nhanh chóng trở thành một trong những chủ đề được thảo luận nhiều nhất tại các hội nghị hành pháp và tư pháp hình sự. Mối quan tâm chưa từng có này đã thúc đẩy cơ quan thực thi pháp luật tạo ra các cơ chế và quy trình để điều tra tội phạm xảy ra trên Darkweb. Tuy nhiên, không có sự tham gia nhất quán ở khu vực Đông Nam Á, do đó, làm giảm hoạt động hợp tác quốc tế và tăng cơ hội cho tội phạm mạng trong khu vực.

Sự gia tăng về số lượt tìm kiếm trên Google về Darkweb cho thấy sự quan tâm ngày càng tăng của công chúng đối với chủ đề này.

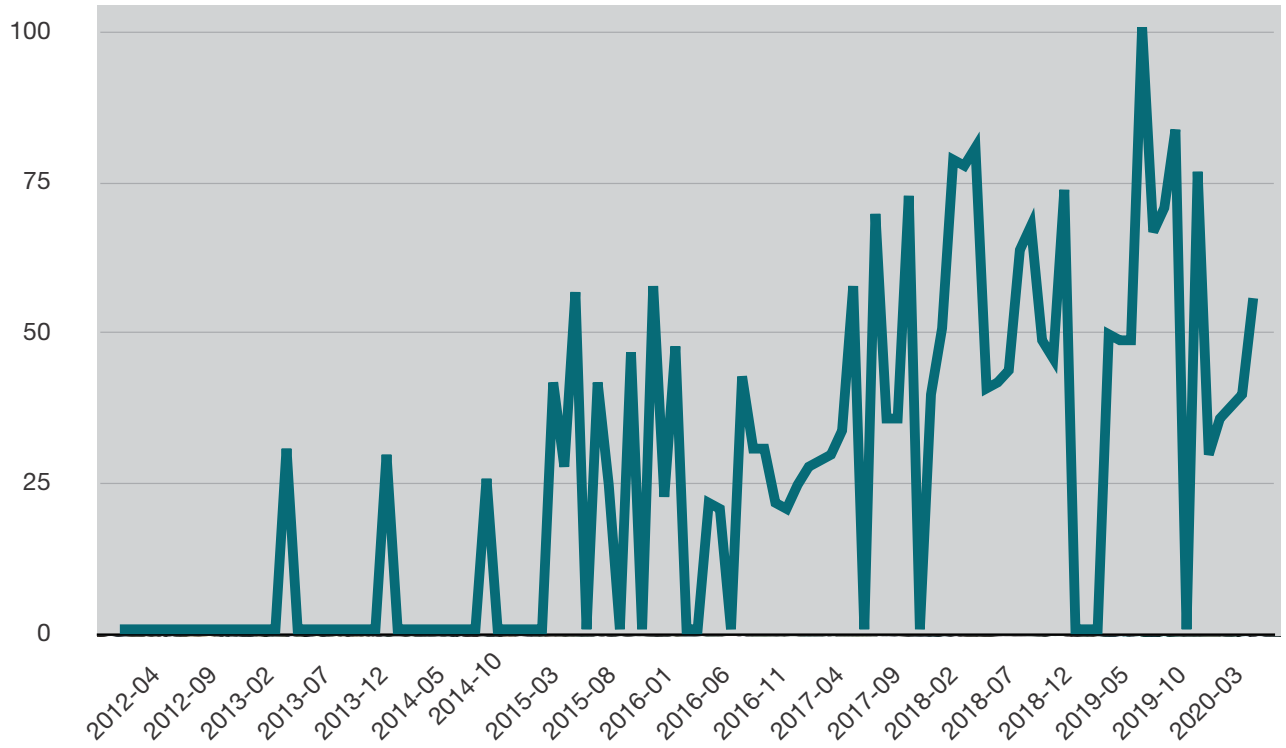
Hình 5. Số lượt tìm kiếm trên Google về Darkweb (tháng 1 năm 2012 đến tháng 7 năm 2020).*



**Dữ liệu từ dịch vụ Google Trends.Các con số thể hiện sở thích tìm kiếm so với điểm cao nhất trên bảng dữ liệu của Đông Nam Á theo thời gian. Giá trị 100 là mức độ phổ biến cao nhất của thuật ngữ, trong khi giá trị 50 có nghĩa là thuật ngữ đó chỉ phổ biến bằng một nửa.*

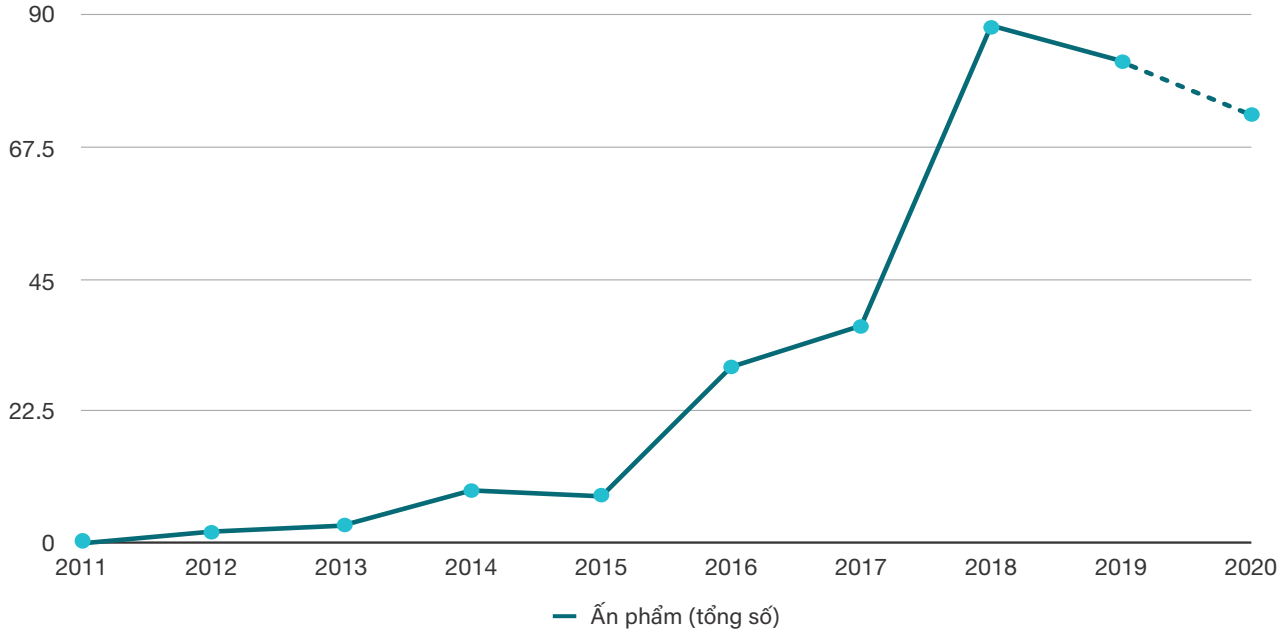
Giới truyền thông đã không bỏ qua xu hướng ngày càng tăng của tội phạm liên quan đến Darkweb này. Do đó, kể từ năm 2014 trở về sau tin tức được đưa thường xuyên hơn.

Hình 6. Số lượng các bài báo ở Đông Nam Á đề cập đến Darkweb (từ tháng 1 năm 2014 đến tháng 7 năm 2020).



Số lượng các bài báo học thuật được xuất bản về Darkweb đã tăng gấp ba lần kể từ năm 2015 (***Hình 7***). Nhiều bài báo khoa học phân tích nội dung của Darkweb và cách sử dụng các công cụ ẩn danh. Tài liệu học thuật năm 2019/2020 bao gồm các hành vi vi phạm về tiết lộ thông tin và dữ liệu có sẵn trên Darkweb và có khả năng giải quyết tác động của đại dịch COVID-19 vào năm 2020/2021.Các ấn phẩm này phân tích dữ liệu từ các thị trường Darkweb, các diễn đàn thảo luận và các nền tảng rò rỉ thông tin (được gọi là "các trang dán").

Hình 7. Số lượng các bài báo khoa học đã xuất bản về Darkweb và darknet.



Sự phổ biến của darknet (đặc biệt là Tor) ngày càng tăng cao trên toàn thế giới. Tuy nhiên, như chúng ta sẽ thấy trong phần tiếp theo, người dùng ở Đông Nam Á dường như chỉ chiếm một tỷ lệ vừa phải trong tổng số.

Darknet ở Đông Nam Á

Bối cảnh

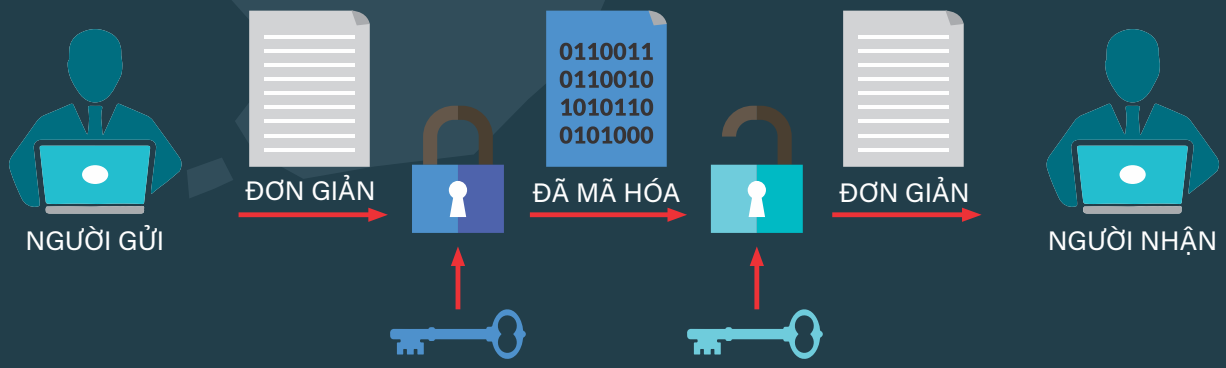
Ở Đông Nam Á, công chúng chủ yếu nghe về Darkweb trên tin tức và qua phương tiện truyền thông xã hội. Theo đánh giá, chỉ có một số ít người đã từng trực tiếp sử dụng nó (xem *A1: Sử dụng Darknet tại các quốc gia Đông Nam Á* trong phần Phụ lục). Ngay cả trên tin tức, Darkweb thường không được thảo luận chi tiết, với hầu hết các câu chuyện liên quan đến việc bắt giữ những tên tội phạm mạng đã sử dụng Darkweb theo một cách nào đó.

Các vụ bắt giữ liên quan đến Darkweb ở Đông Nam Á đã giúp tập trung sự chú ý vào cách các nhóm và tổ chức tội phạm có tổ chức xuyên quốc gia hoạt động trong khu vực. Các giao dịch bất hợp pháp thường là những giao dịch xuyên biên giới, nhấn mạnh nhu cầu hợp tác quốc tế, khả năng tương tác và hiểu biết lẫn nhau về mối đe dọa. Để giúp phát hiện, điều tra, truy tố và ngăn chặn loại tội phạm mạng này, việc nâng cao năng lực của cơ quan thực thi pháp luật là rất quan trọng.

Tội phạm tìm cách ẩn danh bằng cách che giấu hoạt động và danh tính của chúng bằng các phương pháp kỹ thuật như mã hóa và các phương tiện phi kỹ thuật như giao tiếp bằng tiếng Anh thay vì tiếng mẹ đẻ. Rất khó để xác định nơi ở của những thủ phạm cụ thể chỉ dựa vào thông tin giao tiếp của chúng vì nhiều thị trường Darkweb lớn nhất cung cấp dịch vụ và sản phẩm trên toàn thế giới. Như được minh họa trong *Hình 8*, một số ngôn ngữ của Đông Nam Á được sử dụng ít phổ biến hơn. Có những trường hợp mà các trang web dành cho nhiều thị trường cụ thể hơn (xem *Hình 9* cho biết một diễn đàn của Việt Nam về Tor darknet) nhưng trường hợp này rất hiếm.

Mã hóa

Mã hóa: quá trình mã hóa thông tin thành một dạng thay thế chỉ có thể được 'giải mã' bởi những cá nhân được ủy quyền có mã khóa giải mã.Các mã khóa khác nhau được sử dụng để mã hóa và giải mã tin nhắn.



Các từ khóa khác nhau được sử dụng để mã hóa và giải mã tin nhắn

Hình 8. Tiếng Indonesia, tiếng Thái, tiếng Tagalog và tiếng Việt được sử dụng trên các trang web Darkweb (2016-2019).

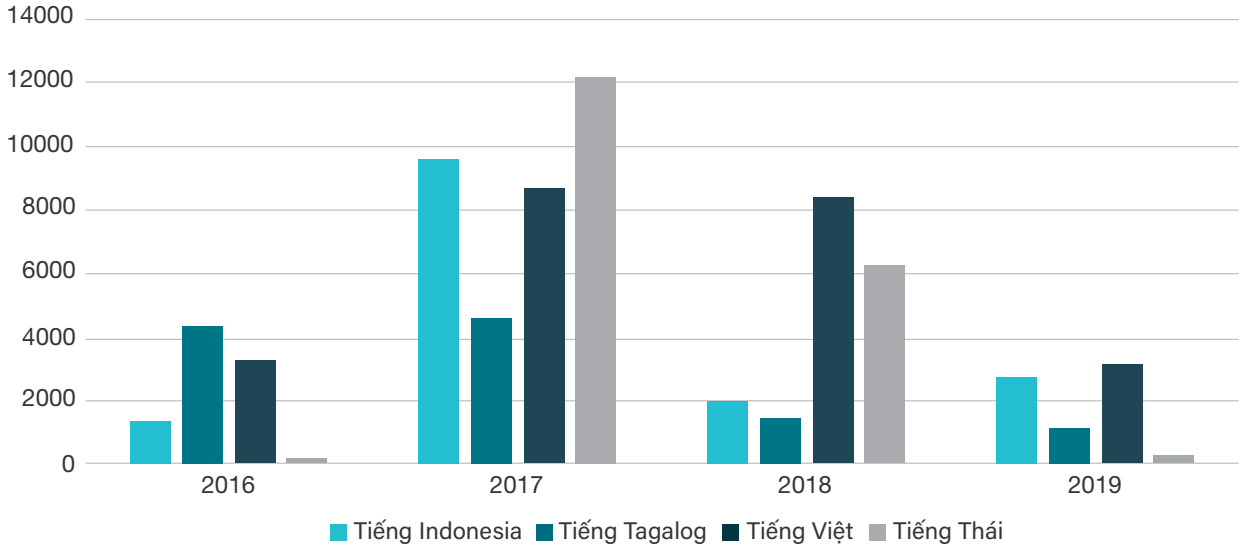
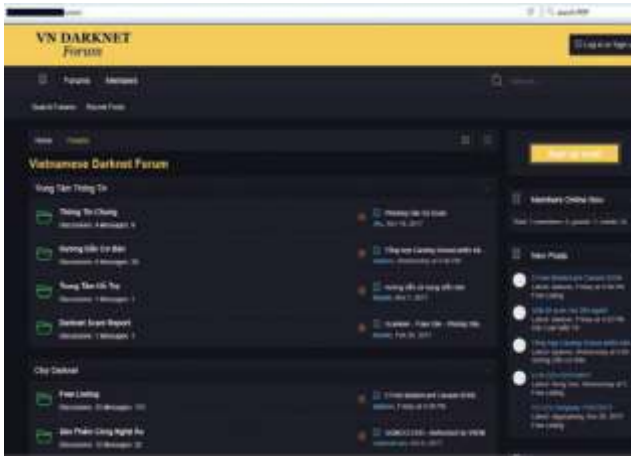


Figure 9. Diễn đàn Darknet của Việt Nam.



Thành công: một phản ứng chắp vá?

Mặc dù bọn tội phạm trên Darkweb luôn nỗ lực để che dấu hành động của chúng, nhưng cơ quan thực thi pháp luật thành đã xác định thành công. Thành công này là nhờ nỗ lực chung của nhiều cơ quan thực thi pháp luật trên toàn thế giới. Khi năng lực điều tra được cải thiện, kết quả hoạt động thành công cũng sẽ được nâng cao.Có thể thực hiện xác định các tác nhân hoặc marketplace riêng lẻ bằng cách phân tích thông tin từ nhiều nguồn. Do đó, điều quan trọng là các quốc gia Đông Nam Á phải tiếp tục hợp tác với các đối tác quốc tế để xây dựng thông tin tình báo có thể thực hiện, lập kế hoạch hành động phối hợp và tìm cách đạt được các kết quả chiến lược chống lại tội phạm mạng có nguy cơ cao nhất.

Ban đầu, điều này yêu cầu phải có một quyết định chính sách giữa các chính phủ để chống lại tội phạm mạng Darkweb (bất kể tình trạng sẵn sàng của các hoạt động trực tuyến trong nước).

Việc liên kết Darkweb với các khu vực pháp lý và ranh giới địa lý cụ thể là một khó khăn về mặt kỹ thuật. Đôi khi phải tiến hành điều tra và truy tố các trường hợp cụ thể để xác định tội phạm đang hoạt động tại các quốc gia nào. Một ví dụ về trường hợp này ở Đông Nam Á, liên quan đến vụ bắt giữ một công dân Canada cư trú tại Thái Lan đang quản lý một marketplace có tên AlphaBay, thị trường lớn nhất trên Darkweb vào năm 2017.

Hoạt động quốc tế nhằm tịch thu cơ sở hạ tầng của AlphaBay có sự hợp tác của các cơ quan thực thi pháp luật ở Thái Lan, Hoa Kỳ, Hà Lan, Lithuania, Canada, Vương quốc Anh và Pháp, cũng như cơ quan thực thi pháp luật châu Âu, Europol[22]. Một trường hợp khác nhấn mạnh bật bản chất của các giao dịch xuyên biên giới. Các giao dịch xuyên biên giới liên quan đến các chuỗi cung ứng toàn cầu, như chuỗi cung ứng bắt nguồn từ Ấn Độ, nơi bọn tội phạm sản xuất ma túy bất hợp pháp để vận chuyển thông qua một tổ chức tội phạm ở Singapore. Từ đó, các bưu kiện tiếp tục hành trình đến Mỹ và Anh[23]. Cả hai trường hợp này đều cho thấy rất cần có những nhân viên tư pháp hình sự có kỹ năng, được trao quyền và một hệ thống hợp tác quốc tế nhanh chóng, trực quan.

Truy tìm những kẻ phạm tội quốc tế có nguy cơ cao nhất: phát trực tiếp

Công nghệ phát trực tuyến càng làm phức tạp thêm vấn đề. Phát trực tiếp trên Darkweb cho phép truyền video, âm thanh và các phương tiện khác để cho phép tội phạm mạng tiếp cận các thị trường từ xa trong thời gian thực. Ví dụ, Peter Gerard Scully, một công dân Úc, đang quản lý một dịch vụ phát trực tiếp từ Philippines, tiếp thị cho những kẻ lạm dụng tình dục trẻ em ở Châu Âu và Hoa Kỳ. Scully bị bắt ở Philippines vào năm 2015 sau khi lạm dụng tình dục một số trẻ em, trong đó có một trẻ sơ sinh 18 tháng tuổi[24]. Cuộc điều tra đã giúp xác định được một nhóm bóc lột tình dục trẻ em quốc tế được cho là đã hãm hiếp, tra tấn, sát hại và phát sóng hành vi ngược đãi các nạn nhân là trẻ em của chúng trên Darkweb cho khách hàng trên khắp thế giới với số tiền lên đến 10.000 đô la Mỹ cho mỗi lượt xem[25]. UNODC đã cố vấn cho các cuộc điều tra tương tự ở nhiều khu vực pháp lý và thừa nhận rằng quy mô và số lượng của các hành vi phạm tội khiến việc truy tố chúng trở nên đặc biệt khó khăn.

Tương tự, vào năm 2018, các nhân viên thực thi pháp luật đã bắt giữ 9 người ở Thái Lan, Úc và Mỹ. Hoạt động đảm bảo an toàn cho 50 trẻ em sau khi các nhà điều tra đánh sập một trang web CSEM Darkweb dựa trên đăng ký với 63.000 người dùng trên toàn thế giới[26].

Rõ ràng rằng hoạt động hợp tác quốc tế là vô cùng quan trọng để cứu các nạn nhân, xác định kẻ phạm tội và ngăn ngừa tổn hại thêm.

Mặc dù có sự hợp tác mạnh mẽ song phương và đa phương, đặc biệt là thông qua các kênh INTERPOL, một số tội phạm vẫn có thể che giấu hành vi phạm tội và danh tính của chúng trong một thời gian dài.

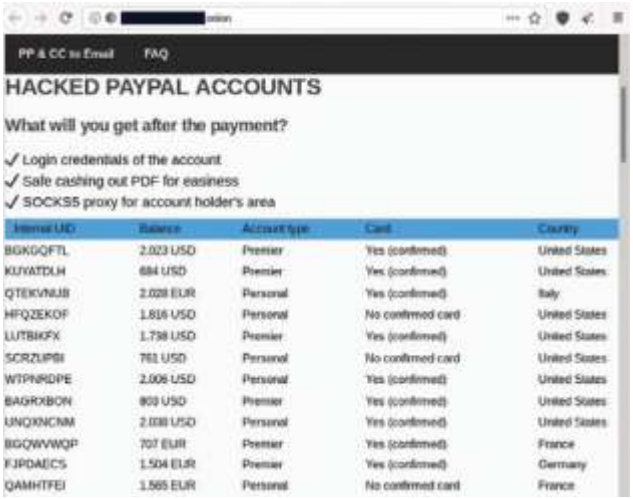
Từ năm 2006 đến năm 2014, Richard Huckle đã lạm dụng tới 200 trẻ em Malaysia và chia sẻ những hình ảnh về tội ác của mình trên Darkweb[27]. Cơ quan Tội phạm Quốc gia của Vương quốc Anh đã bắt giữ Huckle sau khi nhận được thông tin tình báo từ đơn vị bảo vệ trẻ em Argos của Lực lượng Đặc nhiệm Cảnh sát Queensland. Hắn đã bị kết án với 71 tội danh về xâm hại trẻ em từ 6 tháng đến 12 tuổi và nhận 22 bản án chung thân[28].

Những hành vi phạm tội và những kẻ phạm tội này cho thấy hiểm họa rõ ràng và hiện hữu từ những kẻ phạm tội xâm hại tình dục trẻ em phát trực tiếp. Đây là lý do tại sao tất cả các quốc gia cần có một ban lãnh đạo chính sách cấp bộ về các vấn đề mạng để có thể chỉ đạo các nguồn lực cần thiết để đảm bảo an toàn cho những người dễ bị tổn thương nhất trong xã hội.

Lợi nhuận và thua lỗ

Giống như tội phạm thông thường, tội phạm mạng về cơ bản được thúc đẩy bởi lợi nhuận. Tội phạm mạng buôn bán cả thông tin nhận dạng cá nhân và thông tin tài chính bị đánh cắp từ các cá nhân và doanh nghiệp trên các diễn đàn và marketplace của Darkweb. Bọn tội phạm sử dụng thông tin đăng nhập bị đánh cắp (như tên người dùng và mật khẩu) để truy cập vào các dịch vụ trực tuyến và sau đó khai thác thông tin cá nhân của nạn nhân để lừa đảo. Vì thông tin đăng nhập thường vô tình được sử dụng lại, một mật khẩu bị xâm phạm có thể giúp bọn tội phạm có quyền truy cập vào nhiều dịch vụ khác như PayPal (tài khoản PayPal thường được rao bán trên Darkweb – xem *Hình 10*).

Hình 10. Thông tin đăng nhập tài khoản PayPal bị đánh cắp trên Darkweb.*



**Tội phạm mạng bán các thông tin đăng nhập vào tài khoản PayPal bị đánh cắp này không ăn cắp tiền từ tài khoản. Thay vào đó, chúng bán quyền truy cập cho những tội phạm khác, tức là "Tội phạm mạng như một Dịch vụ".*

Một công dân Nga đã bị bắt tại Thái Lan vào năm 2018 vì quản lý marketplace trên Darkweb, Infraud Organization, chuyên bán thông tin thẻ tín dụng bị đánh cắp và phần cứng để xâm nhập cây ATM.

Thị trường có 11.000 thành viên giao dịch hơn 4,3 triệu thẻ tín dụng, thẻ ghi nợ và tài khoản ngân hàng trên toàn thế giới. Điều này khiến những người dùng và doanh nghiệp hợp pháp chịu thiệt hại hơn 530 triệu đô la Mỹ[29]. Tác động của khoản thiệt hại nửa tỷ đô la rất rõ ràng vào thời điểm đó, nhưng trong cuộc suy thoái kinh tế toàn cầu lớn nhất trong 50 năm, tác động của hành vi phạm tội đó đối với sự thịnh vượng kinh tế, sự phục hồi và cuộc sống thực sự là một hiện tượng.

Những ví dụ này cho thấy bọn tội phạm đang hoạt động trên Darkweb ở Đông Nam Á và chống lại các mục tiêu của Đông Nam Á.Cần có một biện pháp ứng phó quốc tế, nhất quán của các cơ quan thực thi pháp luật, được hỗ trợ bởi nhận thức cộng đồng thường xuyên, được quản lý ở cấp bộ tại mỗi quốc gia.

Tác động của đại dịch COVID-19

Đại dịch COVID-19 đã có tác động đến cả hoạt động phạm tội và việc sử dụng Internet nói chung.Mặc dù quá trình thu thập dữ liệu cho báo cáo này được thực hiện trước cuộc khủng hoảng, nhưng điều đáng lưu ý là ở Đông Nam Á, việc sử dụng Tor đã tăng khoảng 20.000 người dùng từ tháng 2 năm 2020[30]. Động cơ thúc đẩy cho điều này không rõ ràng.

Hành vi phạm tội trên Darkweb cũng đã thay đổi. Các diễn đàn Darkweb thường chuyên về buôn bán ma tuý đã bắt đầu cung cấp các mặt hàng liên quan đến COVID-19.Trong đó bao gồm các loại vắc-xin COVID-19 gian lận, hydroxychloroquine và thiết bị bảo vệ cá nhân (xem *Hình 11*). Viện Tội phạm học Úc đánh giá thêm rằng 60% thị trường Darkweb liệt kê ít nhất một sản phẩm liên quan đến COVID-19[31].

Hình 11. Trang web bán hàng hóa liên quan đến COVID-19.

Nhiều hoạt động tội phạm vẫn tiếp tục diễn ra trong thời gian đóng cửa toàn cầu. Thông tin cá nhân tiếp tục bị rò rỉ và rao bán trên Darkweb.Năm 2020, 230.000 hồ sơ bệnh nhân COVID-19 của Indonesia đã bị lộ[32]. Các cuộc tấn công mạng khác đã gia tăng, đặc biệt là các cuộc tấn công của mã độc tống tiền, vì ngày càng có nhiều tổ chức làm việc từ xa. Dữ liệu thu thập từ các nạn nhân được đăng tải trên các diễn đàn Darkweb bằng tiếng Nga và tiếng Anh[33]. Hành vi gian lận trực tuyến, đánh cắp thẻ tín dụng và các cuộc tấn công lừa đảo vẫn tiếp tục diễn ra. Một số trường hợp, như lừa đảo, đã gia tăng và sử dụng các chủ đề COVID-19. Ví dụ, Microsoft đã xác định các email theo chủ đề COVID-19 có chứa một trang tính Excel độc hại.Khi mở ra, các trang tính này sẽ tải xuống phần mềm cho phép kẻ tấn công truy cập từ xa vào máy tính của nạn nhân[34]. Điều này có thể tạo điều kiện cho hành vi phạm tội truyền thống, các cuộc tấn công đe dọa liên tục nâng cao và hành vi của nhà nước thù địch.

Hoạt động Bóc lột Tình dục Trẻ em Trực tuyến (OCSE) cũng gia tăng trong thời kỳ đại dịch với việc cơ quan thực thi pháp luật ở Thái Lan kêu gọi thêm nguồn lực và đào tạo về điều tra OCSE được hỗ trợ bằng Darkweb và tiền điện tử[35]. Hơn nữa, Trung tâm Quốc gia về Trẻ em Mất tích và Bị bóc lột (NCMEC) của Hoa Kỳ đã ghi nhận mức tăng 106% trong các báo cáo về tài liệu về bóc lột tình dục trẻ em khả nghi trên Clearnet - tăng từ 983.734 báo cáo vào tháng 3 năm 2019 lên 2.027.520 vào tháng 5 năm 2020[36]. Phần lớn nội dung lạm dụng được tạo ra sẽ được giao dịch và bán trên Darkweb.

Dù vậy, một số nhóm tội phạm mạng có tổ chức đang bị ảnh hưởng tiêu cực do lệnh đóng cửa. Theo Chainalysis, một công ty phân tích blockchain, có sự sụt giảm 33% về khối lượng lừa đảo tiền điện tử kể từ khi bắt đầu lệnh đóng cửa[37].

Rõ ràng là hành vi phạm tội liên quan đến COVID trên Darkweb chỉ mới bắt đầu. Các quốc gia, đặc biệt là ở Đông Nam Á, phải chú ý đến yêu cầu lập kế hoạch và chuẩn bị, dưới sự chỉ đạo của một ban quản lý cấp bộ về các vấn đề mạng, đối với việc gia tăng tội phạm darknet. Hiện không phải là lúc để giảm đầu tư vào điều tra tội phạm phức tạp, mà là tăng cường nguồn lực, thái độ hoạt động và hợp tác quốc tế. Đó là điều mà công chúng cần và yêu cầu.

Cấu trúc Darkweb và lĩnh vực phạm tội: tìm hiểu thêm

Phần này của báo cáo cung cấp thông tin chi tiết và ví dụ về các thị trường darknet cụ thể và cách hoạt động của tội phạm mạng có liên quan.

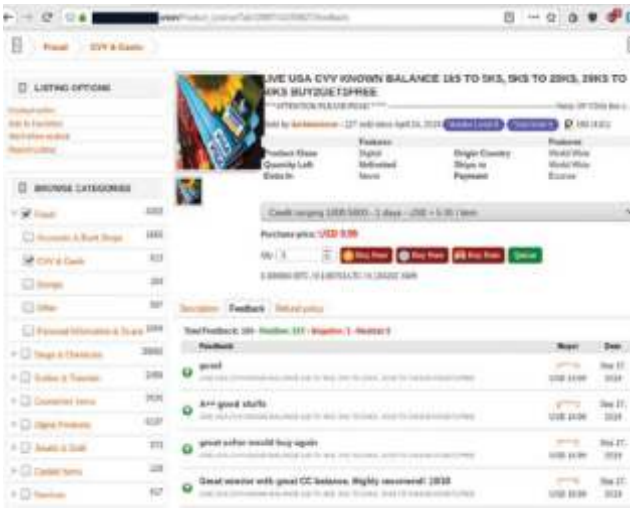
A. Marketplace bất hợp pháp

Do việc sử dụng công nghệ ẩn danh ngày càng tăng, các thị trường darknet bất hợp pháp đã trở nên dễ tiếp cận và phổ biến hơn[38]. Sau khi Bitcoin được giới thiệu vào năm 2009, nó nhanh chóng được chấp nhận như một phương thức thanh toán tại các thị trường chợ đen. Đáng chú ý nhất là vào năm 2011, Silk Road market, một trang web Onion cung cấp nền tảng mua bán các sản phẩm bất hợp pháp (chủ yếu là ma túy), bắt đầu hoạt động bên trong mạng Tor bằng cách sử dụng Bitcoin làm phương thức thanh toán chính (mặc dù ngày nay việc sử dụng các đồng tiền riêng, như Monero và Ethereum đang tăng lên[39]. Silk Road lần đầu tiên kết hợp những công nghệ này để mở ra thị trường trực tuyến cho các sản phẩm bất hợp pháp phát triển mạnh.

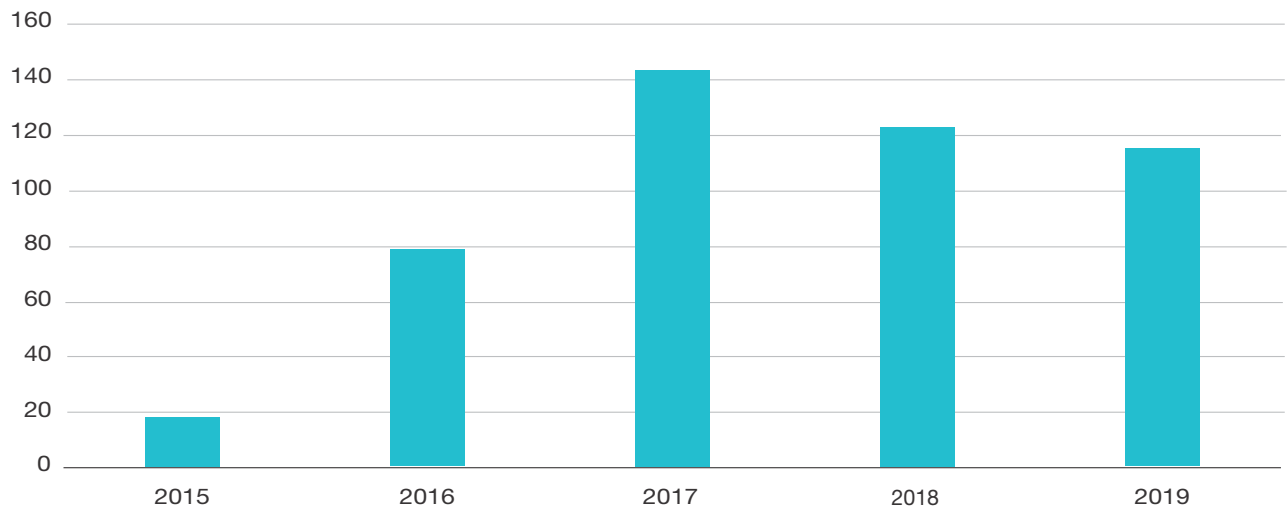
Những marketplace này không phát minh ra công nghệ mới, mà là kết hợp nhiều cải tiến khác nhau để mang lại lợi ích mới cho cả người bán và người mua. Nhờ tính ẩn danh rộng rãi của chúng, tiền điện tử đã trở thành phương tiện để tài trợ cho tội phạm mạng trên Darkweb.

Số lượng marketplace đang hoạt động trên Darkweb đã tăng từ một (Silk Road) vào năm 2011 lên 118 vào năm 2019. Các thị trường này đang cạnh tranh với nhau và phần lớn người dùng sẽ chỉ sử dụng thị trường phổ biến nhất vì ít có nguy cơ lừa đảo hơn.Với sự thống trị của các marketplace lớn này, nhiều thị trường nhỏ hơn không có được khách hàng mới.

Hình 12. Empire Market – một trong những thị trường trực tuyến lớn nhất về các sản phẩm và dịch vụ bất hợp pháp.



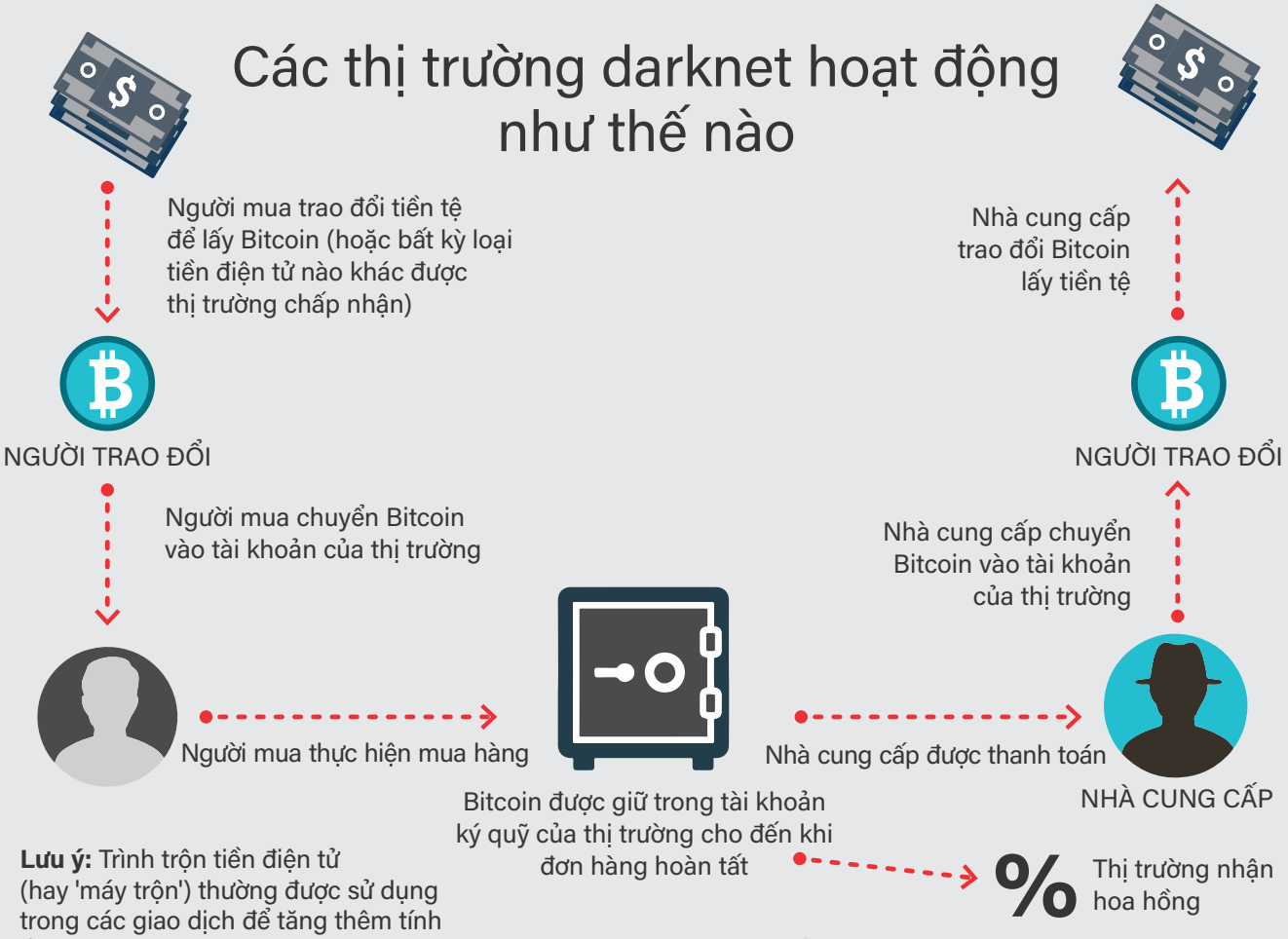
Hình 13. Số lượng thị trường bất hợp pháp đang hoạt động trên Darkweb.



Các thị trường bất hợp pháp được ẩn danh, nhưng bản thân giao dịch lại được hiển thị. Có một số hạn chế quyền truy cập và do đó, về mặt lý thuyết, bất kỳ ai cũng có thể truy cập vào các trang web Onion này và duyệt qua các sản phẩm. Do đó, nhân viên thực thi pháp luật phải giám sát các hoạt động bất hợp pháp bằng cách sử dụng tính năng thu thập thông tin web (quy trình tự động truy cập trang web và lưu nội dung) và công nghệ thu thập dữ liệu (trích xuất thông tin có liên quan từ nội dung để phân tích dữ liệu). Silk Road là một nơi lý tưởng để bắt đầu nghiên cứu sâu hơn về cách các công nghệ truyền thông trực tuyến biến đổi hành vi phạm tội[40]. Bằng cách thu thập thông tin web, bạn có thể theo dõi một số hoạt động trực tuyến của tội phạm trong thời gian thực. Do đó, một số nhà nghiên cứu đã công bố nghiên cứu về các khía cạnh khác nhau của việc buôn bán ma túy bất hợp pháp[41,42,43].

Những marketplace này hoạt động giống như các trang web thương mại điện tử thông thường ngoại trừ việc đó là những hàng hóa và dịch vụ bất hợp pháp được mua và bán[44,45].

Nhìn chung, các marketplace có hệ thống phản hồi và uy tín để phân biệt giữa người bán và người mua được cho là có uy tín dựa trên phản hồi từ các giao dịch trước đó. Tuy nhiên, với cả hoạt động mua và bán, rất khó để xác định tính xác thực của phản hồi vì tất cả các bên về cơ bản đều ẩn danh[46]. Tuy nhiên, điều này cho phép các nhà điều tra theo dõi người bán theo thời gian, trên khắp các thị trường, vì họ cần duy trì tên người dùng và danh tiếng của mình trên tất cả các nền tảng. Cơ quan thực thi pháp luật đang tiến hành loại bỏ các thị trường darknet, nhưng điều đó không có nghĩa là sẽ làm giảm số lượng người dùng/người bán. Khi một thị trường bị loại bỏ, người bán và người mua thường chuyển sang thị trường lớn nhất tiếp theo. Theo quan sát, người bán thậm chí còn sử dụng tên người dùng tương tự khi họ chuyển đến các marketplace khác; ví dụ, bắt đầu trên Silk Road, sau đó chuyển sang AlphaBay, rồi đến các lần chuyển đổi gần đây hơn. Điều này cho thấy sự gián đoạn không nhất thiết giải quyết được vấn đề.



Nguồn: Phỏng theo bằng chứng được đưa vào hồ sơ xét xử liên bang của Ross Ulbricht tại Tòa án Quận phía Nam của New York, Hoa Kỳ, mô tả sơ đồ hệ thống thanh toán của Silk Road theo hình dung của Chính phủ Hoa Kỳ.

Các yếu tố cơ bản của thị trường darknet

Marketplace hoặc thị trường darknet ẩn danh cần bốn thành phần để hoạt động:

1. Một nền tảng ẩn danh, chống kiểm duyệt để hoạt động, ví dụ: một trang web Onion.
2. Hệ thống tiền tệ ẩn danh (bán ẩn danh) trực tuyến, như Bitcoin.
3. Một hệ thống thanh toán ký quỹ (kế toán ký quỹ nội bộ).
4. Uy tín và phản hồi (chỉ số uy tín minh bạch).

Khi bốn công nghệ này được kết hợp và sử dụng đồng thời, thị trường darknet có thể hoạt động hiệu quả. Nếu không có một trong các thành phần này, thị trường sẽ ngừng hoạt động[47].

Với các tính năng như hệ thống thanh toán ký quỹ và chỉ số uy tín/phản hồi, khả năng người mua sẽ nhận được sản phẩm họ đã mua (và thông tin sản phẩm hợp lệ) đã tăng lên. Nhiều người bán cố gắng cung cấp thông tin sản phẩm chính xác và phản hồi tích lũy xác minh tuyên bố của người bán[48,49].

Khi giao dịch đã diễn ra trực tuyến, nhà cung cấp có thể giao hàng trên toàn thế giới thông qua bất kỳ số lượng dịch vụ gửi qua đường bưu điện nào. Khi nói đến mua ma túy, việc mua bán trực tuyến được coi là an toàn hơn mua ngoài đường, nơi có nguy cơ bạo lực và cướp giật[50,51]. Không cần tiếp xúc trực tiếp với người bán và dễ dàng có được thông tin chính xác về sản phẩm[52,53].

Người mua thường sẽ mua một số loại tiền ảo (thường là Bitcoin), tạo tài khoản trên marketplace, chuyển bitcoin vào ví trong tài khoản của họ, sau đó chọn một sản phẩm để mua. Nếu mặt hàng được chọn là sản phẩm thực, như hộ chiếu giả hoặc ma túy bất hợp pháp, thì người mua cung cấp thông tin giao hàng cho người bán. Hệ thống ký quỹ khóa số tiền thanh toán từ ví của người mua. Tiếp theo, người bán gửi sản phẩm và người mua đưa ra phản hồi công khai (tích cực hoặc tiêu cực) cho người bán. Sau hành động đó, hệ thống ký quỹ sẽ chuyển khoản thanh toán cho người bán.

Việc đưa ra ý kiến phản hồi liên quan đến giao dịch rất quan trọng đối với người bán vì những người mua trong tương lai có nhiều khả năng chọn những người bán đáng tin cậy đã nhận được những phản hồi tích cực. Những nhà cung cấp tạo dựng được danh tiếng tốt, để cung cấp dịch vụ chất lượng cao có thể tạo dựng tên tuổi cho chính mình và sau đó hoạt động trong các thị trường khác nhau bằng cách sử dụng tên tương tự.

B. Tiền điện tử

Sau khi Bitcoin (loại tiền điện tử đầu tiên) được giới thiệu vào năm 2009, nó nhanh chóng được sử dụng như một phương thức thanh toán tại các thị trường chợ đen. Bất kể những người ẩn danh tin Bitcoin là thế nào, các giao dịch vẫn để lại dấu vết trong Bitcoin blockchain. Blockchain là một hồ sơ giao dịch công khai cho biết tất cả các giao dịch giữa các ví Bitcoin. Hầu hết các sàn giao dịch Bitcoin trực tuyến đều đã bắt đầu yêu cầu giấy tờ nhận dạng trước khi một người có thể mua bitcoin, có nghĩa là có thể truy xuất danh tính của người mua và nơi bitcoin được gửi đến theo mặc định. Do đó, hiện có các dịch vụ để che giấu bất kỳ dấu vết kỹ thuật số nào liên quan đến các giao dịch bất hợp pháp. Chúng thường được gọi là trình trộn tiền điện tử, máy trộn hoặc dịch vụ giặt là.

Các dịch vụ này hoạt động bằng cách trộn các bitcoin đến vào một nhóm với các bitcoin ngẫu nhiên khác được giữ trong kho dự trữ, sau đó xuất ra các bitcoin khác không có liên quan đến bitcoin sắp tới. Quá trình trộn này phá vỡ mối liên hệ giữa giao dịch mua bitcoin ban đầu và điểm thanh toán, do đó việc đưa kẻ phạm tội ra trước công lý bằng cách "theo dõi tiền" trở nên khó khăn hơn.

Bổ sung thêm tính ẩn danh bằng cách sử dụng cái gọi là "trình trộn kép". Quy trình trộn hai giai đoạn này, được thực hiện trong trình duyệt web, bổ sung thêm một mức ẩn danh khác vì không trình trộn nào biết cả nguồn và điểm đến của bitcoin. Trang web này tạo điều kiện cho quy trình trộn nhưng không tìm hiểu các địa chỉ đã sử dụng. Tuy nhiên, nếu một trong những trình trộn không an toàn hoặc bị xâm nhập, thì khả năng ẩn danh có thể bị mất. Một rủi ro nữa là các trình trộn được sử dụng trong quá trình này có thể có khả năng đánh cắp bitcoin.

Tiền điện tử

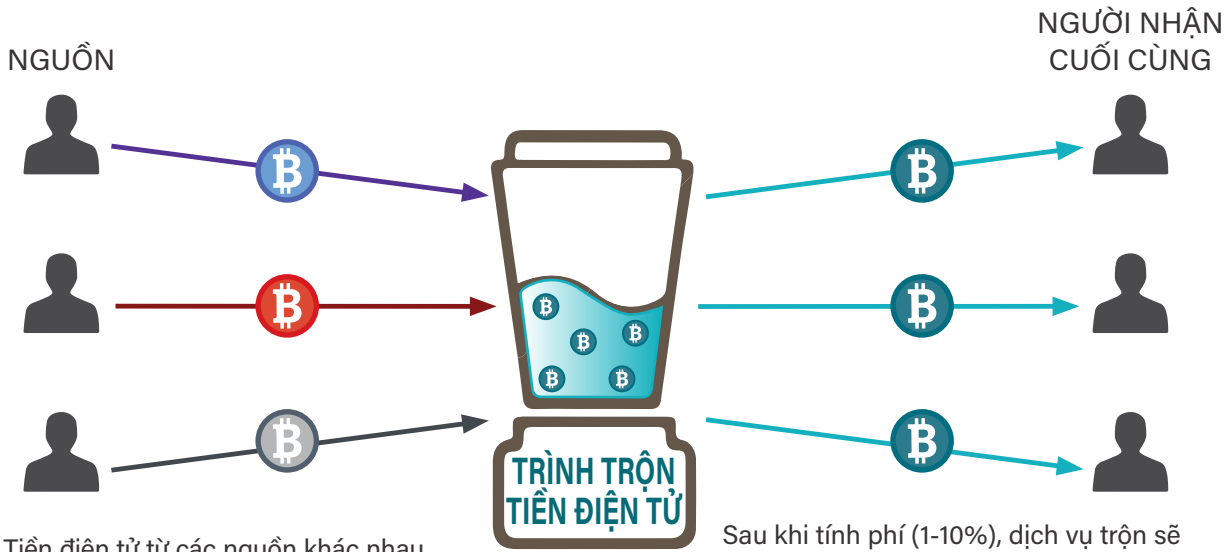
Thông tin nhanh

- Tiền điện tử là một dạng tài sản ảo dựa trên một mạng được phân phối trên một số lượng lớn các máy tính. Cấu trúc phi tập trung này cho phép chúng tồn tại ngoài tầm kiểm soát của các chính phủ và chính quyền trung ương.
- Một số kỹ thuật mã hóa được sử dụng trong tiền điện tử ngày nay ban đầu được phát triển cho các ứng dụng quân sự. Về mặt nào đó, các chính phủ muốn kiểm soát kỹ thuật mã hóa, nhưng người dân được đảm bảo quyền sử dụng nó dựa trên cơ sở tự do ngôn luận.
- 'Blockchains' (các phương pháp tổ chức để đảm bảo tính toàn vẹn của dữ liệu giao dịch) là một thành phần thiết yếu của nhiều loại tiền điện tử. Nhiều chuyên gia tin rằng blockchain và công nghệ có liên quan sẽ làm xáo trộn nhiều ngành trong tương lai, bao gồm cả tài chính và luật.
- Tiền điện tử gặp phải những lời chỉ trích vì một số lý do, như việc sử dụng chúng cho các hoạt động bất hợp pháp, biến động tỷ giá hối đoái và các lỗ hổng của cơ sở hạ tầng sử dụng chúng. Tuy nhiên, chúng cũng được khen ngợi vì tính linh động, khả năng phân chia, khả năng chống lạm phát và tính minh bạch.
- Tiền điện tử dựa trên blockchain đầu tiên là Bitcoin, hiện vẫn là loại tiền điện tử phổ biến nhất và có giá trị nhất.Tính đến tháng 11 năm 2019, đã có hơn 18 triệu bitcoin được lưu hành với tổng giá trị thị trường khoảng 146 tỷ đô la Mỹ.
- Ngày nay, tổng giá trị của tất cả các loại tiền điện tử đang tồn tại là khoảng 214 tỷ đô la Mỹ- Bitcoin hiện chiếm hơn 68% tổng giá trị.

Nguồn: www.investopedia.com (Tiền điện tử)

Trình trộn tiền điện tử

Trình trộn tiền điện tử: các dịch vụ nhận token tiền điện tử có thể nhận dạng từ một ví và xuất token 'sạch' không thể nhận dạng sang một ví (hoặc các ví khác).



Tiền điện tử từ các nguồn khác nhau được gửi đến trình trộn.

Sau khi tính phí (1-10%), dịch vụ trộn sẽ gửi tiền điện tử 'đã trộn' đến bất cứ nơi nào được yêu cầu. Liên kết đến nguồn hiện sẽ bị phá vỡ.

Các dịch vụ trộn này không được đăng ký với tư cách là công ty. Chúng hoạt động mà không cần giấy phép để xử lý các giao dịch tài chính và có thể vi phạm luật chống rửa tiền, chống tài trợ khủng bố và các lệnh trừng phạt của Hội đồng Bảo an Liên hợp quốc. Các dịch vụ trao đổi Bitcoin được cấp phép có thể cố gắng tránh chuyển trực tiếp đến các địa chỉ ví đã biết của các dịch vụ trộn.

Hình 14. Trang web của DoubleMixer trên mạng Tor.

Bitcoin không phải là phương thức thanh toán duy nhất có sẵn. Có các loại tiền điện tử khác, được gọi là tiền riêng, được sử dụng trong giao dịch bất hợp pháp như Monero, Litecoin, Bitcoin Cash, Ethereum và Dash.

Monero đã thu hút tội phạm mạng vì nó cung cấp mức độ ẩn danh cao hơn cho các giao dịch. Monero tạo địa chỉ duy nhất cho mọi giao dịch và chỉ người nhận mới có thể truy cập đầy đủ thông tin giao dịch. Monero cũng thực hiện trộn tự động và gây khó khăn cho việc theo dõi các giao dịch trên blockchain của họ.

Hình 15. Lời khuyên thanh toán cho người dùng trang web trên marketplace Cannazon. *

**Trang web khuyên bạn nên sử dụng Monero thay vì Bitcoin vì Monero cung cấp khả năng ẩn danh giao dịch cao hơn. Khi sử dụng Bitcoin, bạn nên sử dụng dịch vụ trộn ('lộn tiền của bạn').*

Lần đầu tiên được giới thiệu làm phương thức thanh toán bởi các marketplace AlphaBay và Oasis, Monero đã được các thị trường Darkweb lớn chấp nhận kể từ năm 2016. Mặc dù vậy, Bitcoin vẫn chiếm ưu thế trong giao dịch bất hợp pháp và hầu hết các thị trường chỉ sử dụng Bitcoin như một phương thức thanh toán. Điều này được minh họa trong *Bảng 1* ở trang sau cho biết các tùy chọn thanh toán được 40 marketplace phổ biến chấp nhận trên Darkweb. Theo dự đoán, đồng tiền riêng, theo thời gian, sẽ trở thành phương thức thanh toán chính cho hàng hóa bất hợp pháp.

Bảng 1. Các tùy chọn thanh toán trên 40 marketplace Darkweb tính đến tháng 12 năm 2019.

Tên marketplace	Bitcoin	Monero	Litecoin	Bitcoin Cash	Ethereum	Dash
Empire Market	Bitcoin	Monero	Litecoin			
Hydramarket	Bitcoin					
Apollon Market	Bitcoin	Monero	Litecoin	Bitcoin Cash		
Genesis Market	Bitcoin					
BitMarket	Bitcoin					
Brians Club Market	Bitcoin		Litecoin			
Cannazon market	Bitcoin	Monero				
Alpha Omega Market	Bitcoin					
Ali Marketplace	Bitcoin					
Sipulimarket	Bitcoin					
Icarus Market	Bitcoin	Monero				
DeepSea Market	Bitcoin					
Elite Market	Bitcoin					
Grey Market	Bitcoin	Monero				
Samara Market	Bitcoin	Monero		Bitcoin Cash		
Berlusconi Market	Bitcoin	Monero	Litecoin			
DarkMarket	Bitcoin	Monero				
White House Market		Monero				
Luna Market	Bitcoin					
Silk Road 4	Bitcoin	Monero	Litecoin		Ethereum	
Midland City	Bitcoin					
Point Market	Bitcoin			Bitcoin Cash	Ethereum	
Dr. Bob	Bitcoin					
CanonZone	Bitcoin	Monero				
The French Connection	Bitcoin					
Dutch Drugs	Bitcoin	Monero	Litecoin		Ethereum	Dash
CharlieUK	Bitcoin					
Cannabis Grower	Bitcoin					
Glass Werkz	Bitcoin					
ElHerbolario's Shop	Bitcoin					
Cocaine Market	Bitcoin					
Dutch Magic	Bitcoin					
Pushing Taboo	Bitcoin					
Global Dreams	Bitcoin					
Evil Shop	Bitcoin					
Yakuza Market	Bitcoin	Monero				
Weedstore	Bitcoin					
Rsclub Market	Bitcoin					
Hidden Marketplace	Bitcoin					
HookShop	Bitcoin					

Theo *Bảng 1*, gần như mọi marketplace đều sử dụng Bitcoin làm phương thức thanh toán - ngoại lệ duy nhất là White House Market chỉ chấp nhận Monero. Monero có sẵn như một phương thức thanh toán ở một phần ba các marketplace phổ biến này và thường được khuyên dùng vì tính ẩn danh mà nó cung cấp mà không cần dịch vụ trộn riêng. Litecoin có sẵn ở 17,5% thị trường. Các phương thức thanh toán khác được hỗ trợ là Bitcoin Cash (khác với Bitcoin), Ethereum và Dash, nhưng chỉ bởi một số marketplace.

Là loại tiền được chấp nhận rộng rãi nhất trên các marketplace Darkweb, Bitcoin có thể được truy cập dễ dàng và nhanh chóng thông qua các sàn giao dịch và các giao dịch không dễ dàng được truy xuất nếu sử dụng dịch vụ trộn.

Monero cũng có bán qua một số sàn giao dịch, nhưng không phải tất cả, như sàn giao dịch tiền điện tử lớn, Coinbase, không hỗ trợ Monero. Năm 2020, Coinbase cung cấp 30 loại tiền điện tử khác nhau để giao dịch nhưng không bao gồm Monero. Tuy nhiên, Monero dự kiến sẽ trở nên phổ biến hơn trên các marketplace Darkweb vì nó cung cấp tính năng ẩn danh theo mặc định.

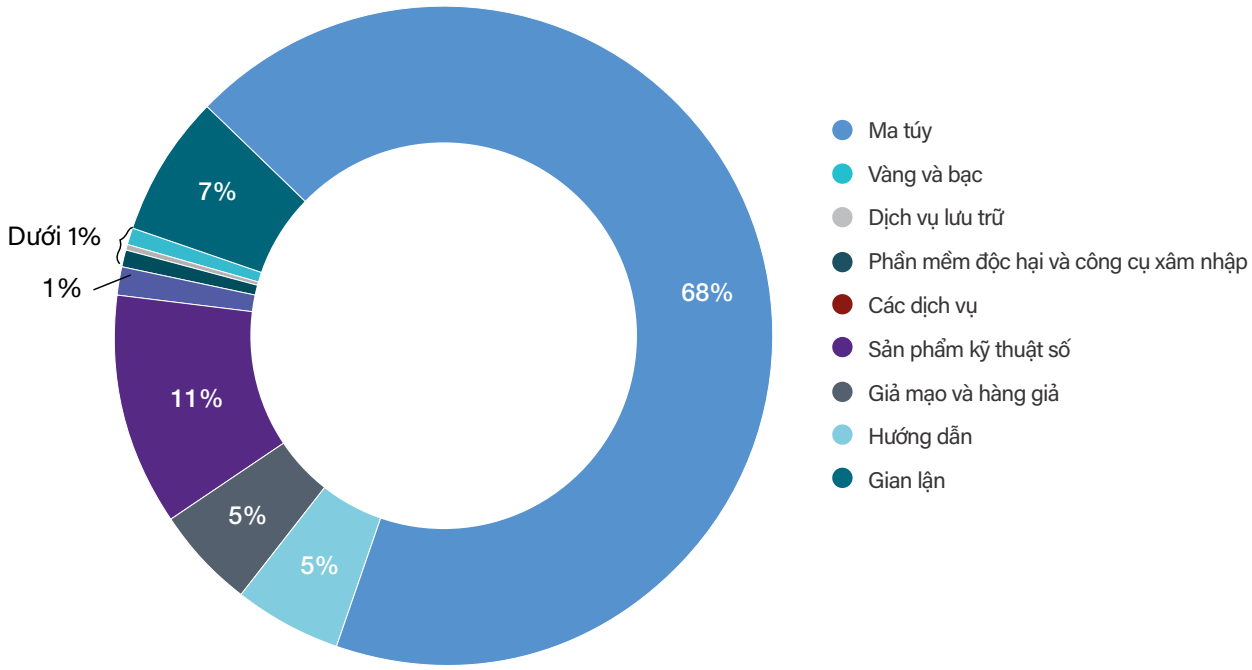
C. Các sản phẩm và dịch vụ bất hợp pháp

Có rất nhiều sản phẩm và dịch vụ bất hợp pháp trên Darkweb. Phần này xem xét các sản phẩm và dịch vụ bất hợp pháp có trên mạng Tor.

Dữ liệu tổng hợp từ bốn marketplace Darkweb (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) cho thấy ma túy là loại sản phẩm bất hợp pháp phổ biến nhất có tại các marketplace này (68%). Tiếp theo là các sản phẩm kỹ thuật số (12%) bao gồm các trò chơi, phần mềm vi phạm bản quyền và các mã khóa cấp phép có liên quan; sau đó là các mặt hàng giả mạo (7%) bao gồm thông tin thẻ thanh toán, thông tin cá nhân và thông tin đăng nhập bị đánh cắp; tiếp theo là các mặt hàng giả (5%) bao gồm tiền, đồ điện tử, hộ chiếu và giấy phép lái xe.

Tài liệu có bản quyền cũng được chia sẻ trên Darkweb. Cái được gọi là các trang BitTorrent (torrent) trong mạng Tor chứa các tệp torrent cho phép người dùng tải xuống các bộ phim, bản nhạc và trò chơi một cách bất hợp pháp.

Hình 16. Tỷ lệ các sản phẩm và dịch vụ có trên marketplace Darkweb tính đến tháng 12 năm 2019.*

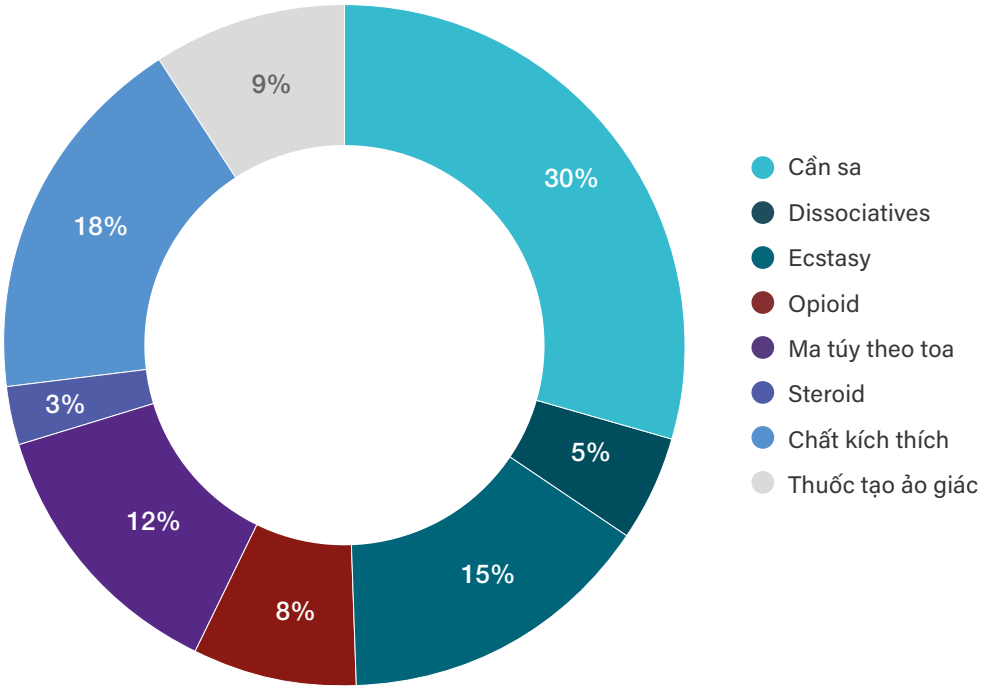


**Dữ liệu tổng hợp từ bốn marketplace phổ biến (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) cho thấy ma túy là danh mục sản phẩm phổ biến nhất hiện có trên các marketplace này tính đến tháng 12 năm 2019.*

1. Ma túy

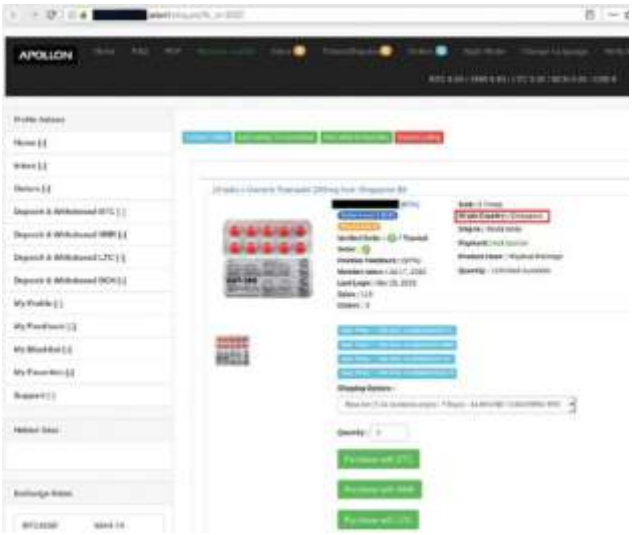
Danh mục sản phẩm được giao dịch rộng rãi nhất trên Tor darknet là ma túy. Tổng số mặt hàng được bày bán trên bốn thị marketplace mục tiêu vào tháng 12 năm 2019 là 138.405 và trong số này có 94.389 mặt hàng là ma túy. Các loại ma túy bao gồm MDMA, amphetamine, methamphetamine, cần sa ở mọi hình thức, cocaine, opioid ở mọi hình thức, LSD, nấm ảo giác, ketamine và ma túy theo toa (chủ yếu là benzodiazepine).

Hình 17. Tỷ lệ các loại ma túy có trên bốn marketplace phổ biến vào tháng 12 năm 2019.*



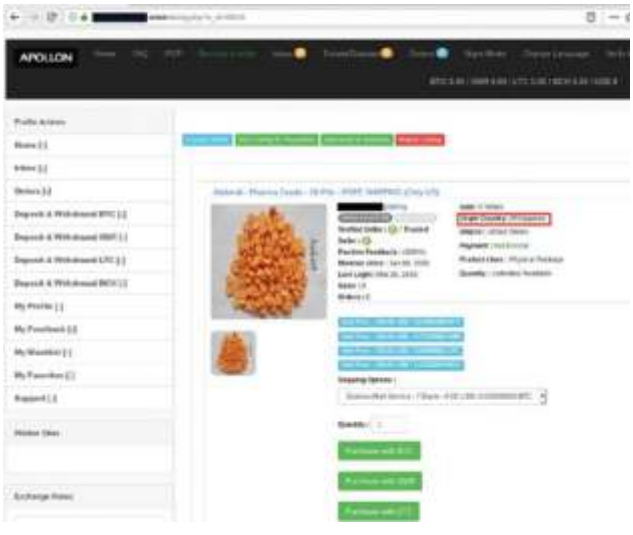
Dữ liệu tổng hợp từ bốn marketplace phổ biến (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) tính đến tháng 12 năm 2019.

Hình 18. Ví dụ về trang web bán ma túy trên Darkweb.*



Cho thấy nhà cung cấp gửi ma túy từ Singapore đến bất kỳ nơi nào trên thế giới.

Hình 19.Ví dụ về việc mua bán mua túy bất hợp pháp trên Darkweb.*



Cho thấy một nhà cung cấp gửi các sản phẩm từ Philippines đến Hoa Kỳ.

2. Gian lận thẻ thanh toán

Việc buôn bán thông tin tài chính bị xâm phạm trên Darkweb là một ví dụ về tội phạm mạng như một dịch vụ (CaaS).Gian lận thẻ thanh toán nghĩa là việc lấy và sử dụng trái phép dữ liệu thẻ thanh toán, như số thẻ, địa chỉ thanh toán, mã bảo mật và ngày hết hạn, để mua sản phẩm[54]. Trong hầu hết các trường hợp, nạn nhân không biết về hành vi sử dụng trái phép thẻ của họ.

Ví dụ, các cuộc tấn công phi kỹ thuật lừa nạn nhân tiết lộ thẻ và thông tin cá nhân của họ. Nạn nhân có thể cung cấp thông tin của họ mà không biết rằng trang web hoặc đại diện dịch vụ khách hàng thực sự là một kẻ lừa đảo.Loại hoạt động bất hợp pháp này đã phát triển ổn định với thông tin thẻ bị đánh cắp bằng cách sử dụng các hành vi vi phạm dữ liệu, tấn công phi kỹ thuật (các hoạt động độc hại được thực hiện thông qua tương tác của con người), phần mềm độc hại đánh cắp dữ liệu và các công cụ lừa đảo (rất nhiều trong số đó hiện có sẵn trên các diễn đàn, marketplace và cửa hàng thẻ tự động)[55]. Các vụ tội phạm xâm nhập vào các công ty và đánh cắp cơ sở dữ liệu thông tin thẻ tín dụng lớn (thường xâm nhập hàng triệu tài khoản trong quá trình này) đang trở nên phổ biến hơn.

Hình 20. Nhà cung cấp cung cấp dịch vụ thẻ giả nhằm vào khu vực Đông Nam Á.

Hình 21. Thông tin thẻ tín dụng Malaysia được giao bán trên Darkweb.

Web skimming là một phương pháp gian lận thẻ khác. Trang thanh toán trên một trang web bị xâm phạm khi tội phạm cài đặt phần mềm độc hại trên trang đó, qua đó đánh cắp thông tin thanh toán của nạn nhân.

Trên Darkweb, có bán các hướng dẫn và công cụ về cách xâm nhập các thiết bị và hệ thống thanh toán thẻ. Điều này thường diễn ra tại điểm bán hàng (PoS), nơi mọi người thực hiện các giao dịch thanh toán. Hệ thống PoS bao gồm một thiết bị đọc thông tin thẻ và phần mềm PoS trong máy tính để gửi dữ liệu thanh toán đến nhà cung cấp dịch vụ thanh toán. Các công cụ phần mềm độc hại được bán trên Darkweb có thể được cài đặt trên hệ thống PoS, cho phép kẻ tấn công thu thập dữ liệu thẻ trong quá trình xử lý thanh toán.

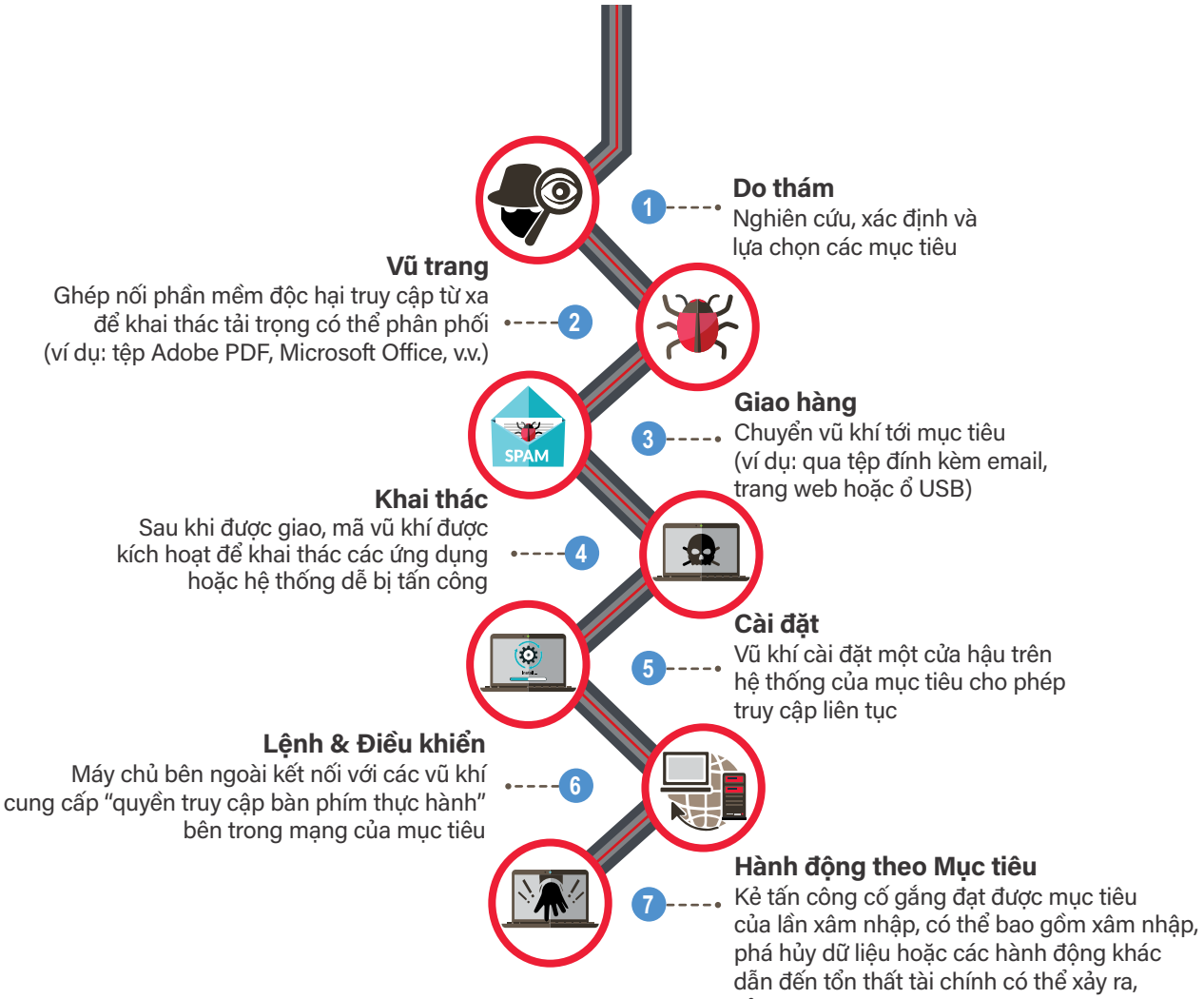
Thông tin thẻ tín dụng được thu thập có thể được sử dụng để thanh toán gian lận hoặc bán có kỳ hạn. Trên các marketplace Darkweb, có rất nhiều bộ sưu tập thông tin thẻ tín dụng được rao bán mà bọn tội phạm có thể mua để rút tiền mặt hoặc thực hiện các giao dịch gian lận. Những rủi ro về sự ổn định và thịnh vượng của nền kinh tế là rất rõ ràng.

3. Phần mềm độc hại như một dịch vụ

Các lập trình viên có chuyên môn cao có thể xây dựng các chương trình máy tính và mạng có khả năng phát động các cuộc tấn công mạng chống lại các tổ chức. Đó là loại phần mềm được phát triển thành các bộ công cụ và mạng robot (botnet) được bán như một dịch vụ trên Darkweb. Đây được gọi là "phần mềm độc hại như một dịch vụ" (MaaS). MaaS cho phép các chuyên gia không chuyên về mạng mua phần mềm và sau đó sử dụng phần mềm đó để lây nhiễm phần mềm độc hại vào hệ thống và kiểm soát các hệ thống đó để sử dụng bất hợp pháp. Trên thực tế, bọn tội phạm mua các công cụ này để có quyền truy cập vào các vectơ tấn công xâm nhập, phức tạp, mà đôi khi chúng không thể kiểm soát được sau khi triển khai. Ngay cả những chuyên gia có trình độ chuyên môn cao cũng gặp phải khó khăn này – như đã thấy trong các kịch bản WannaCry và NotPetya năm 2017. Những rủi ro do một cuộc tấn công mạng không được kiểm soát gây ra vượt xa tác động của tội phạm mạng truyền thống. Có thể dẫn đến xung đột và thậm chí là chiến tranh. Do đó, điều cần thiết là các Quốc gia phải có một ban quản lý cấp bộ về các vấn đề mạng, người có thể tham gia ở cấp cao nhất trong hoạt động ngoại giao không gian mạng phòng ngừa ở ASEAN, Đại hội đồng LHQ và Hội đồng Bảo an LHQ.

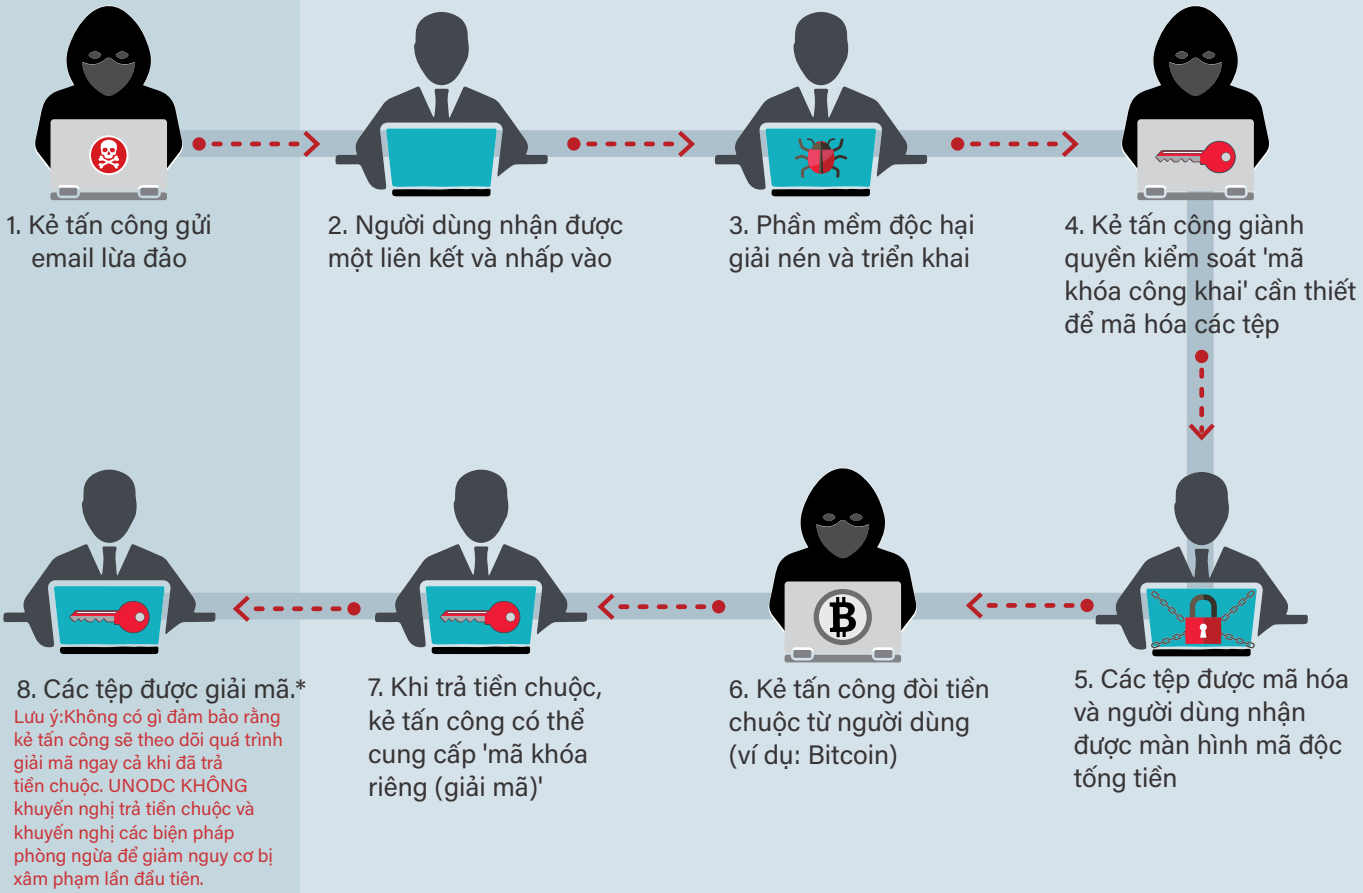
Cách những kẻ tấn công mạng thực hiện tấn công

Tấn công mạng: hành vi cố ý khai thác hệ thống máy tính và mạng để chiếm đoạt hoặc gây thiệt hại cho nạn nhân.



Nguồn: Phỏng theo Cyber Kill Chain® do Lockheed Martin phát triển.

Phân tích một cuộc tấn công bằng mã độc tống tiền



Mã độc tống tiền như một Dịch vụ (RaaS): biện pháp cung cấp mã độc tống tiền và hệ thống kiểm soát của nó cho khách hàng để sử dụng vào mục đích phạm tội. Tất cả các khía cạnh của việc tạo và kiểm soát mã độc tống tiền có thể được cung cấp như một dịch vụ để mua. Khách hàng có thể lựa chọn các dịch vụ mà họ cần theo phương thức gọi món.

Nguồn: Phỏng theo Centrify Corporations

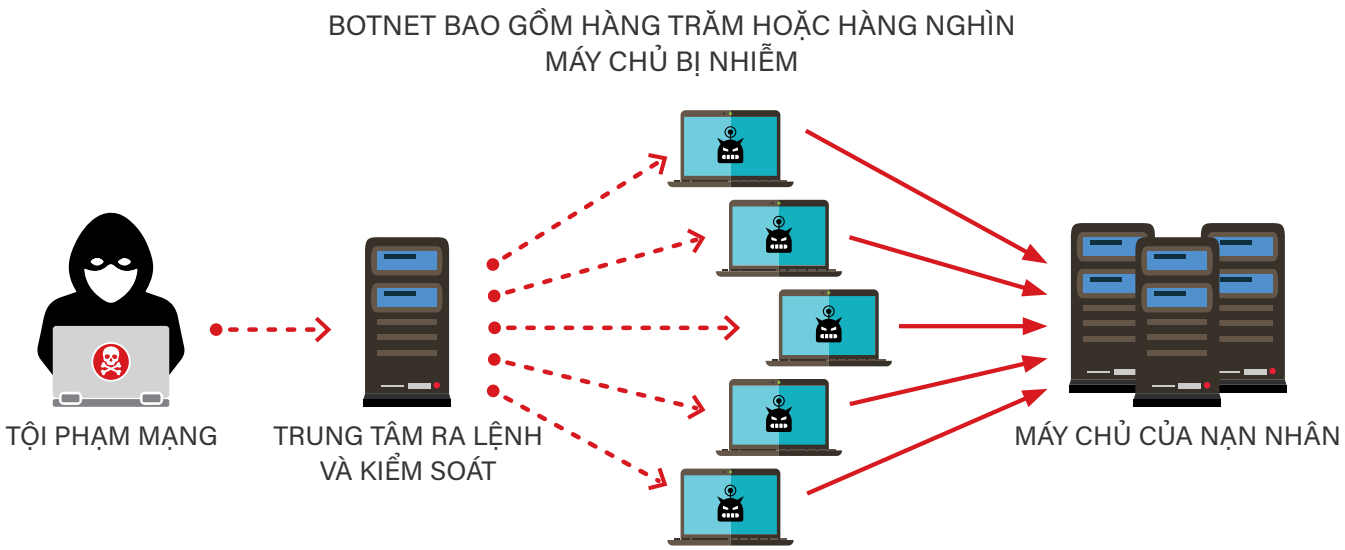
4. Mã độc tống tiền

Mã độc tống tiền là một loại phần mềm độc hại lấy dữ liệu làm con tin. Tội phạm sử dụng mã độc tống tiền để ngăn nạn nhân mục tiêu truy cập vào dữ liệu của họ, sau đó đe dọa công bố dữ liệu của nạn nhân hoặc khai thác chúng theo một cách nào đó trừ khi nạn nhân trả tiền chuộc.

Đôi khi nạn nhân của các cuộc tấn công bằng mã độc tống tiền được hướng dẫn trả tiền chuộc thông qua trang web Darkweb, thường bằng tiền điện tử, do đó việc theo dõi điểm đến của các khoản tiền trở nên khó khăn hơn. Các nhà cung cấp Darkweb cũng bán các công cụ mã độc tống tiền và mạng phân phối chỉ làm trầm trọng thêm vấn đề và sự gia tăng của mã độc tống tiền.

Tấn công từ chối dịch vụ (DDoS) phân tán

DDoS: một cuộc tấn công mạng sử dụng một mạng máy tính phân tán để lấn át tài nguyên của hệ thống mục tiêu đến mức mục tiêu không thể tiếp tục hoạt động bình thường.



1. Kẻ tấn công gửi các lệnh "khởi chạy" đến một mạng botnet từ một máy chủ ra lệnh và kiểm soát.

2. Bots gửi lưu lượng tấn công đến máy chủ của nạn nhân.

3. Lưu lượng tấn công lấn át máy chủ, khiến nó không thể đáp ứng các yêu cầu phù hợp.

Nguồn: Phỏng theo F5 Labs (Application Threat Intelligence)

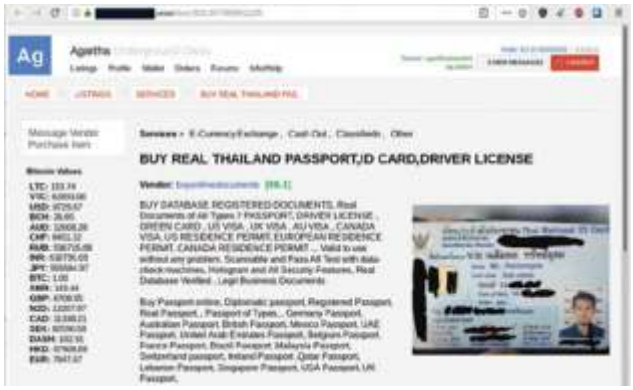
5. Từ chối dịch vụ

Từ chối dịch vụ (DoS) là một cuộc tấn công vào một dịch vụ làm gián đoạn chức năng bình thường của nó và ngăn người khác truy cập. Đây thường là một cuộc tấn công vào một dịch vụ trực tuyến như một trang web, mặc dù các cuộc tấn công cũng có thể được thực hiện với toàn bộ mạng. Bọn tội phạm bán các cuộc tấn công DoS như một dịch vụ trên Darkweb. Điều này thường liên quan đến việc lây nhiễm phần mềm độc hại cho một số lượng lớn máy tính, sau đó sử dụng mạng botnet này để phát động các cuộc tấn công DoS. Chính chủ sở hữu của các mạng botnet này đã bán các khả năng DoS thông qua các marketplace Darkweb. Người mua cũng có thể thuê khả năng của các mạng botnet để xử lý một dịch vụ trực tuyến cụ thể. Người mua cung cấp thông tin chi tiết về dịch vụ mục tiêu cho nhà cung cấp, sau đó trả tiền mỗi giờ để nhà cung cấp thực hiện cuộc tấn công DoS. Một cuộc tấn công từ chối dịch vụ (DDoS) phân tán là một cuộc tấn công trong đó các mạng botnet lấn át dịch vụ mục tiêu bằng nhiều lưu lượng truy cập hơn mức mà máy chủ hoặc mạng có thể đáp ứng, khiến chúng gặp sự cố.

6. Giả mạo

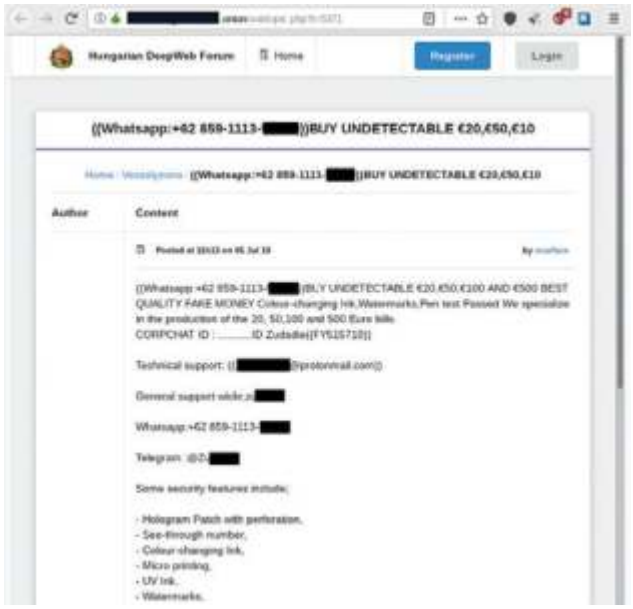
Giả mạo là một dịch vụ phổ biến khác được cung cấp trên Darkweb và thường liên quan chặt chẽ đến hành vi trộm cắp danh tính. Trên Darkweb, bọn tội phạm buôn bán hộ chiếu, giấy phép lái xe và tiền giả. Quyền truy cập thông tin cá nhân sẽ hỗ trợ việc giả mạo giấy tờ tùy thân cũng đang được rao bán. Giấy tờ giả và dịch vụ giả mạo phổ biến trên Darkweb, chiếm 5% tổng giao dịch tại các marketplace phổ biến nhất.Tất nhiên, những giấy tờ giả mạo này thường được mua để che giấu danh tính thực của tội phạm khi chúng thực hiện các vụ phạm tội khác.

Hình 22. Nhà cung cấp bán nhiều loại giấy tờ giả và bị đánh cắp.*



**Cũng như nhiều loại giấy tờ giả, nhà cung cấp này đang bán hộ chiếu, thẻ căn cước và bằng lái xe "thật" từ Thái Lan.*

Hình 23.Nhà cung cấp bán tiền giả.*



7. Trang web lừa đảo

Không có gì ngạc nhiên khi Darkweb ẩn danh là nơi có nhiều kẻ lừa đảo. Hành vi lừa đảo bao gồm các trang web và diễn đàn yêu cầu thanh toán trước bằng Bitcoin cho các sản phẩm và dịch vụ của họ. Không có gì đảm bảo rằng sản phẩm hoặc dịch vụ sẽ được giao và rất ít cơ hội được hoàn lại tiền nếu người mua không hài lòng với sản phẩm của mình. Giữa năm 2020, nhiều trang web Darkweb tuyên bố đang bán vắc-xin hoặc thuốc điều trị virus corona trong đại dịch COVID-19. Các trang web này yêu cầu thanh toán trước và không bao giờ cung cấp sản phẩm như đã hứa.

Một loại hành vi lừa đảo khác xảy ra trên Darkweb là "exit scam". Hành vi này xảy ra khi một marketplace đột ngột đóng cửa mà không có cảnh báo, mang theo tất cả bitcoin hiện được lưu vào ví của người dùng trang web. Các nhà cung cấp cũng có thể ngừng cung cấp các sản phẩm hoặc dịch vụ của họ và trốn thoát với tất cả số bitcoin được thanh toán cho các đơn đặt hàng chưa được giao.

8. Diễn đàn xâm nhập

Diễn đàn hacker là các diễn đàn không đồng bộ được tạo ra và hoạt động chủ yếu để thảo luận về các chủ đề liên quan đến xâm nhập. Các chủ đề được quan tâm trong các diễn đàn này bao gồm từ tin tức và hướng dẫn chung về bảo mật máy tính cho đến việc phát tán phần mềm độc hại và thông tin bị rò rỉ. Các diễn đàn này cũng thảo luận và chia sẻ các thủ thuật ẩn danh, các công cụ xâm nhập máy chủ và các kỹ thuật bẻ khóa mật khẩu.

Hình 24. Một nhà cung cấp cung cấp nhiều loại dịch vụ xâm nhập.

Các diễn đàn và kênh thảo luận thường được sử dụng trên Darkweb để điều phối các cuộc tấn công, chia sẻ các công cụ tấn công và để trao đổi thông tin chung về các chủ đề liên quan đến các hoạt động bất hợp pháp.

9. Tiết lộ thông tin nhận dạng và không nhận dạng cá nhân

Một hoạt động phổ biến của tội phạm mạng là chia sẻ dữ liệu bị vi phạm như mật khẩu, tài liệu bảo mật, cơ sở dữ liệu và thông tin tài chính. Dữ liệu này thường được khai thác bởi bọn tội phạm tiến hành các cuộc tấn công mạng diễn ra bên ngoài Darkweb.

Rò rỉ dữ liệu trái phép không nhất thiết có nghĩa là một tổ chức là nạn nhân của hành vi xâm nhập gây hại. Trên thực tế, phần lớn các sự cố rò rỉ dữ liệu được cho là vô tình. Ví dụ, một nhân viên có thể vô tình gửi email đến nhầm người hoặc cấp nhầm cho người ngoài quyền truy cập vào hệ thống của công ty. Bất kể động cơ là gì, rò rỉ dữ liệu không chủ ý có thể gây thiệt hại tương tự như hành vi vi phạm cố ý.

Rò rỉ thông tin có chủ ý xảy ra khi kẻ tấn công (từ trong công ty mục tiêu hoặc người ngoài) có được quyền truy cập vào dữ liệu của tổ chức. Tội phạm mạng thường sử dụng phần mềm độc hại đối với nhân viên và máy tính của họ với tỷ lệ thành công cao, nhưng các phương pháp ít yêu cầu thành thạo về kỹ thuật cũng có thể rất hiệu quả, như tội phạm mạng có thể dễ dàng giả mạo tài khoản email doanh nghiệp hợp pháp và yêu cầu bất kỳ số lượng nhân viên nào gửi cho họ thông tin nhạy cảm hoặc bí mật thương mại của công ty.

Thông thường, bọn tội phạm sẽ sao chép và dán dữ liệu bị xâm phạm vào một trang web nền tảng rò rỉ thông tin và công bố dữ liệu theo một tên người dùng duy nhất.Tội phạm mạng chia sẻ tên người dùng này với những tên tội phạm khác để có thể truy cập vào nội dung bất hợp pháp. Đôi khi, nội dung chỉ tồn tại trong một khoảng thời gian ngắn trên trang web dán, do đó hạn chế hiển thị tổng thể. Tuy nhiên, các trang web khác sẽ lưu giữ dữ liệu vô thời hạn. Các diễn đàn Darkweb ngầm thường bị hacker sử dụng để thông báo về các hành vi vi phạm dữ liệu, trước khi chia sẻ hoặc mua bán thông tin. Phân tích và xác định các chủ đề thảo luận trên các diễn đàn này có thể giúp các nạn nhân bị xâm phạm phản ứng kịp thời với các sự cố.

10. Bán quyền truy cập cho các tổ chức

Hacker đôi khi bí mật giữ quyền truy cập vào các máy chủ bị xâm nhập mà tổ chức mục tiêu không hề hay biết.Quyền truy cập này rất có giá trị. Một số nhóm chuyên thu thập quyền truy cập trái phép vào máy chủ, sau đó bán thông tin này cho các nhóm khác, những người chuyên thực hiện các hoạt động trong tổ chức mục tiêu. Các nhóm tội phạm mạng xuyên quốc gia chuyên thu thập quyền truy cập vào các tổ chức mục tiêu có giá trị cao sẽ bán thông tin xác thực truy cập từ xa trên Darkweb. Sau khi nhận được khoản thanh toán, chúng cung cấp hướng dẫn cho người mua về cách truy cập từ xa vào tổ chức mục tiêu.

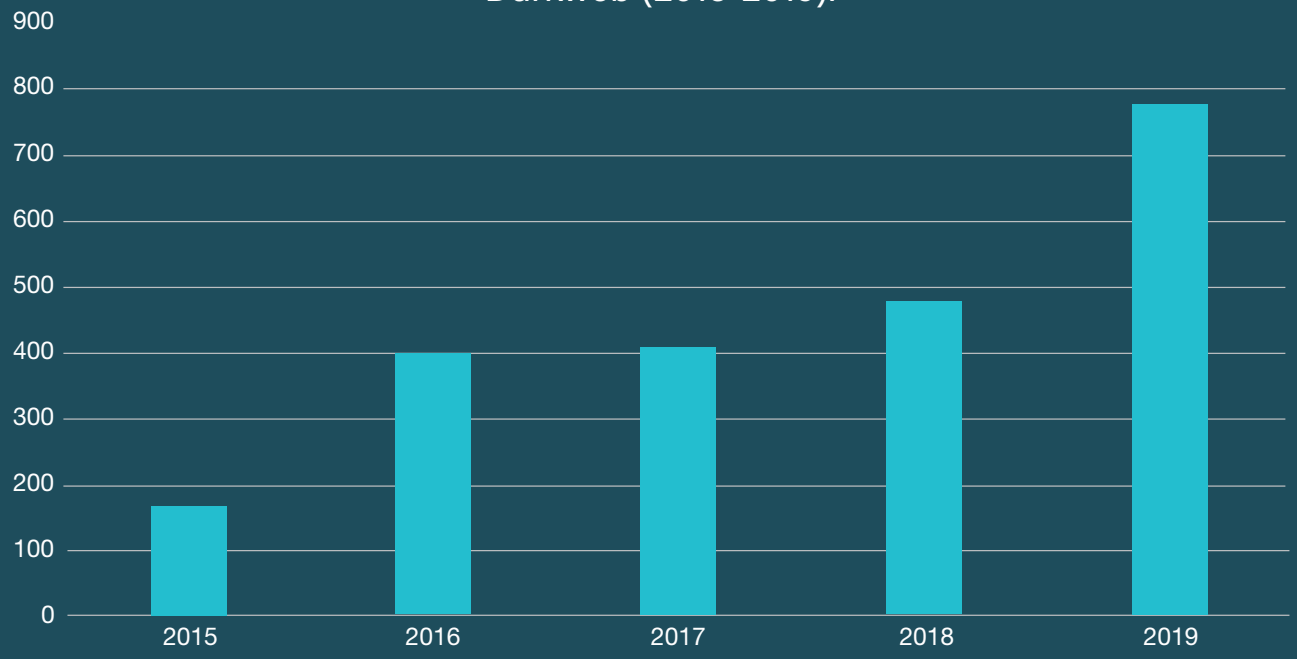
11. Tài liệu về bóc lột tình dục trẻ em

Các diễn đàn Darkweb (và người dùng của chúng) đã lưu trữ, chia sẻ, giao dịch và bán tài liệu bóc lột tình dục trẻ em (CSEM) trong nhiều năm. Số lượng CSEM tăng lên theo thời gian khi nội dung mới được thêm vào và tài liệu cũ được lưu trữ.

Rất khó để xóa nội dung này vĩnh viễn. Các trang web CSEM thường sao chép nội dung từ các trang khác, có nghĩa là khi một trang web bị gỡ xuống, dữ liệu vẫn được lưu trữ trên các trang khác. Với các trang web mới được thiết lập và tài liệu mới được bổ sung liên tục, dịch vụ sẽ được cung cấp liên tục.

Một số trang web thậm chí còn tuyên bố rằng họ đang thu thập một kho lưu trữ tài liệu CSEM để phân phối và quảng cáo có hàng terabyte nội dung. Ngoài ra còn có các trang web bán quyền truy cập vào CSEM – bao gồm cả việc lạm dụng phát trực tiếp trả tiền cho mỗi lần xem, với Bitcoin thường là đơn vị tiền tệ được chọn để thanh toán.

Hình 25. Số lượng các trang web CSEM độc quyền đã công bố trên Darkweb (2015-2019).



Như được minh họa trong *Hình 25*, lượng nội dung CSEM trên Darkweb đang tăng lên nhanh chóng.Trên thực tế, một phân tích sử dụng so sánh nội dung văn bản vào năm 2019 cho thấy có 776 trang web độc quyền chia sẻ CSEM (khoảng 5% trong số 15.353 trang web Onion hiện hoạt)[56]. Mặc dù rất nhiều trang web này đang hoạt động dưới các tên miền onion khác nhau, nhưng nội dung trên nhiều trang web có vẻ giống hệt nhau.

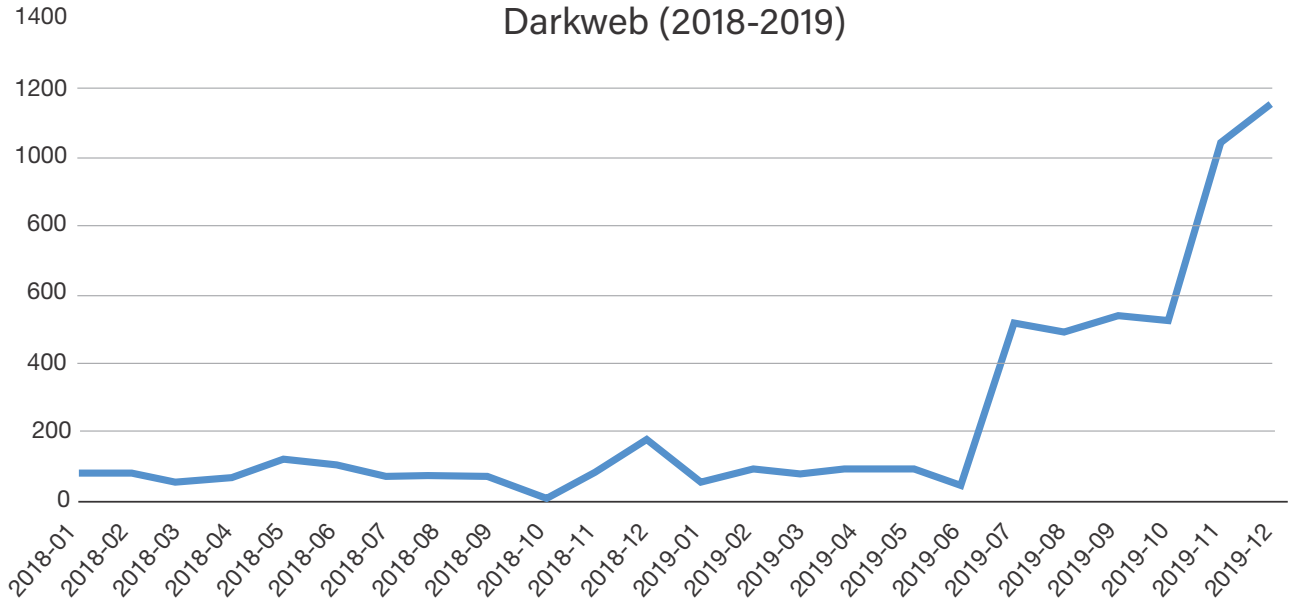
12. Buôn bán động vật hoang dã

Với việc mở rộng thương mại, kéo theo sự xuất hiện của các sản phẩm động vật hoang dã bất hợp pháp trên các thị trường darknet. *Hình 26* cho thấy hoạt động buôn bán sừng tê giác trong năm 2019.

Hình 26. Hoạt động buôn bán động vật hoang dã trái phép diễn ra trong các marketplace Darkweb. *

**Four different vendors selling rhino horns on the Agartha marketplace.*

Hình 27. Số lần "sừng tê giác" được đề cập trên Darkweb (2018-2019)



Kết luận

Mặc dù có rất ít dữ liệu liên quan đến việc nhắm mục tiêu đến tội phạm Darkweb và có nguồn gốc từ Đông Nam Á, nhưng thông tin có sẵn cho thấy tội phạm mạng tồn tại và có khả năng phát triển theo chiều rộng và chiều sâu trong thời gian tới. Đồng thời, đại dịch COVID-19 đã khẳng định rõ ràng rằng bọn tội phạm sẽ phát triển các mô hình kinh doanh của chúng một cách nhanh chóng để tiếp tục tạo ra lợi nhuận lớn nhất có thể. Các quốc gia cũng phải được thúc đẩy để nhanh chóng đánh giá, phân tích và chuyển hướng các nguồn lực hoạt động để ứng phó với các mối đe dọa về tội phạm mạng đang phát triển. Điều cần thiết là các quốc gia Đông Nam Á phải có trách nhiệm riêng để giải quyết các vấn đề chính trị và chính sách tổng thể đặt ra trong việc chống lại tội phạm mạng darknet, nhưng họ cũng cần đầu tư nhanh chóng vào việc nâng cao kỹ năng cho các cơ quan tư pháp hình sự của mình. Tội phạm mạng Darknet không còn là một "ẩn số chưa biết" và cần phải có sự cống hiến, chuyên môn, cố vấn chuyên môn và nguồn lực tài chính để xây dựng năng lực chống lại mối đe dọa. UNODC vẫn cam kết hỗ trợ Đông Nam Á với công việc quan trọng này.

Phụ lục

A1: Sử dụng Darknet tại các quốc gia Đông Nam Á

Bằng cách sử dụng các số liệu được cung cấp bởi hai trong số các darknet (Tor và I2P), có thể biết được số lượng người dùng gần đúng ở mỗi quốc gia Đông Nam Á. Những số liệu này giúp chúng ta hiểu rõ hơn về hành vi của người dùng theo thời gian. Điều quan trọng cần lưu ý là không thể đưa ra kết luận về hành vi phạm tội từ những số liệu này – chúng chỉ đơn giản là để đưa ra bức tranh toàn cảnh về việc sử dụng darknet.

Tor cung cấp hai số liệu hữu ích: người dùng chuyển tiếp và người dùng cầu nối.Người dùng chuyển tiếp là bất kỳ người dùng nào ở một quốc gia cụ thể đang chuyển tiếp lưu lượng truy cập mạng Tor. Người dùng cầu nối là người dùng cuối bị chặn (vì bất kỳ lý do gì) không được truy cập trực tiếp vào mạng Tor. Người dùng cầu nối không có chức năng chuyển tiếp.

I2P cung cấp thông tin định tuyến theo quốc gia. Tương tự như Tor, người dùng kết nối với mạng I2P thông qua bộ định tuyến phần mềm cục bộ. Các bộ định tuyến nhận và chuyển tiếp lưu lượng truy cập I2P từ các nút khác trên mạng I2P. I2P duy trì số lượng bộ định tuyến hiện hoạt cho mỗi quốc gia trong tối đa một năm.

Ngoài ra còn có các phương pháp khác để người dùng kết nối với darknet, điều này gây khó khăn cho việc phân bổ số lượng chính xác người dùng cho các quốc gia cụ thể. Ví dụ: người dùng ở quốc gia A có thể sử dụng VPN hoặc dịch vụ tương tự để kết nối với quốc gia B. Trong khi có vẻ như ở quốc gia B, người dùng lại kết nối với mạng Tor. Tor sẽ đăng ký người dùng là kết nối từ quốc gia B. Do đó, chúng tôi phải đưa ra kết luận rằng số lượng người dùng được chỉ ra trong các số liệu mạng này có thể không thể hiện đúng số lượng người dùng thực tế.

Dưới đây, chúng tôi cung cấp thông tin tổng quan về người dùng darknet theo quốc gia đối với mạng Tor và I2P. Trong hầu hết các biểu đồ, có sự tăng vọt về số lượng người dùng trong năm 2013 và 2018. Cả hai đợt tăng vọt này có thể do phần mềm độc hại đã kết nối các hệ thống bị nhiễm với mạng Tor gây ra[57].

1. Brunei Darussalam

Brunei có dân số khoảng 440.000[58]. Số liệu Tor (*Hình A1*) cho thấy việc sử dụng Tor đã giảm từ mức trung bình 500 người được kết nối mỗi ngày trong vài năm qua xuống mức trung bình 250 người được kết nối vào năm 2020. Giống như nhiều quốc gia khác, chúng tôi nhận thấy sự gia tăng về số lượng người dùng vào đầu năm 2020.

Hình A1. Người dùng Tor được kết nối trực tiếp từ Brunei (tháng 1 năm 2012 đến tháng 7 năm 2020).

Tor Project - https://metrics.torproject.org/

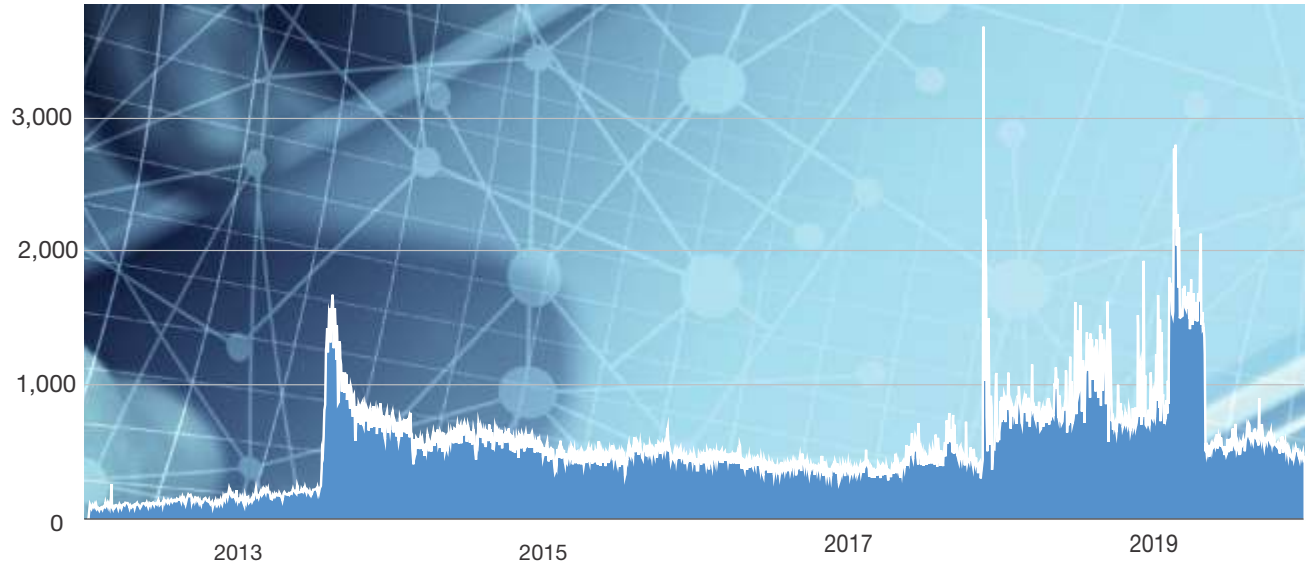
Người dùng cầu nối mạng Tor trung bình cũng có khoảng 10 người dùng được kết nối mỗi ngày. Lưu ý rằng đây có thể là những người dùng cùng kết nối và ngắt kết nối mạng hoặc những người dùng khác nhau. 250 người dùng chuyển tiếp và 10 người dùng cầu nối nên được coi là tổng số người dùng tối thiểu có thể.

Không có hoạt động nào được báo cáo từ Brunei trên darknet I2P từ tháng 1 năm 2019 đến tháng 7 năm 2020. Điều này có nghĩa là I2P đã không được sử dụng trực tiếp.

2. Campuchia

Campuchia có dân số khoảng 16,7 triệu[59]. Số liệu Tor (*Hình A2*) cho thấy việc sử dụng mạng Tor đã tăng từ mức trung bình khoảng 500 người dùng mỗi ngày vào năm 2018 lên mức trung bình là 2.500 người dùng vào cuối năm 2019. Vào đầu năm 2020, chúng tôi chứng kiến sự sụt giảm trở lại mức trung bình 500 người dùng.Sự biến động đó có thể là do nhận thức của người dùng được nâng cao hoặc do chiến dịch phần mềm độc hại hoặc sự kiện kiểm duyệt trong nước[60].

Hình A2. Người dùng Tor được kết nối trực tiếp từ Campuchia (tháng 1 năm 2012 đến tháng 7 năm 2020).



Tor Project - https://metrics.torproject.org/

Vào đầu năm 2018, chúng tôi chứng kiến sự gia tăng lớn về số lượng người dùng cầu nối mạng Tor từ mức trung bình 10 người dùng lên mức trung bình khoảng 700 người dùng. Kể từ đó, người dùng cầu nối đã giảm dần, với mức trung bình khoảng 50 người dùng vào năm 2020.

Không có hoạt động nào được báo cáo từ Campuchia trên darknet I2P từ tháng 1 năm 2019 đến tháng 7 năm 2020. Điều này có nghĩa là I2P đã không được sử dụng trực tiếp.

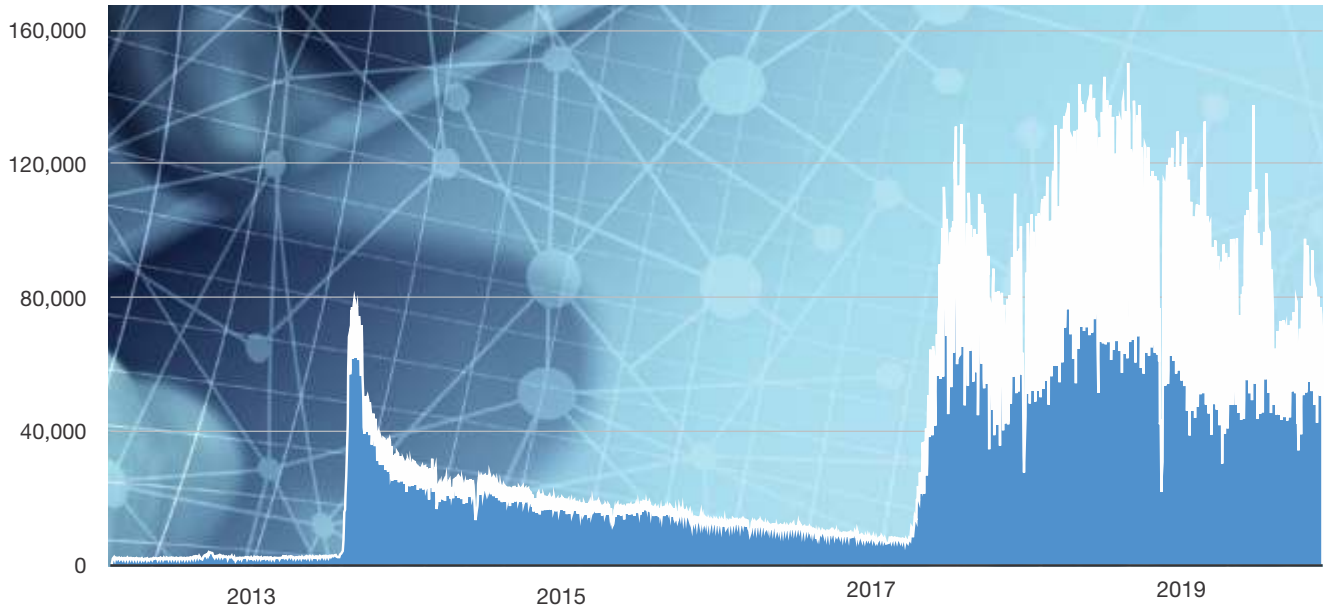
3. IndonesiaIndonesia

có dân số khoảng 274 triệu[61]. Số liệu Tor (*Hình A3*) cho thấy việc sử dụng mạng Tor đã tăng từ mức trung bình khoảng 10.000 người dùng mỗi ngày vào năm 2017 lên mức trung bình là 125.000 người dùng vào cuối năm 2019.Vào đầu năm 2020, chúng tôi chứng kiến sự sụt giảm trở lại mức trung bình 75.000 người dùng.

Vào đầu năm 2018, chúng tôi chứng kiến sự gia tăng lớn về số lượng người dùng cầu nối mạng Tor từ mức trung bình 100 người dùng lên mức trung bình khoảng 12.500 người dùng. Người dùng cầu nối đã giảm đều đặn xuống mức trung bình khoảng 600 người dùng vào năm 2020.

Indonesia có khoảng 150 người dùng I2P vào đầu năm 2019.Con số đó giảm xuống còn khoảng 25 người dùng vào đầu năm 2020 và sau đó tăng lên mức trung bình 50 người dùng trong khoảng thời gian từ tháng 1 đến tháng 7 năm 2020.

Hình A3. Người dùng Tor được kết nối trực tiếp từ Indonesia (tháng 1 năm 2012 đến tháng 7 năm 2020).

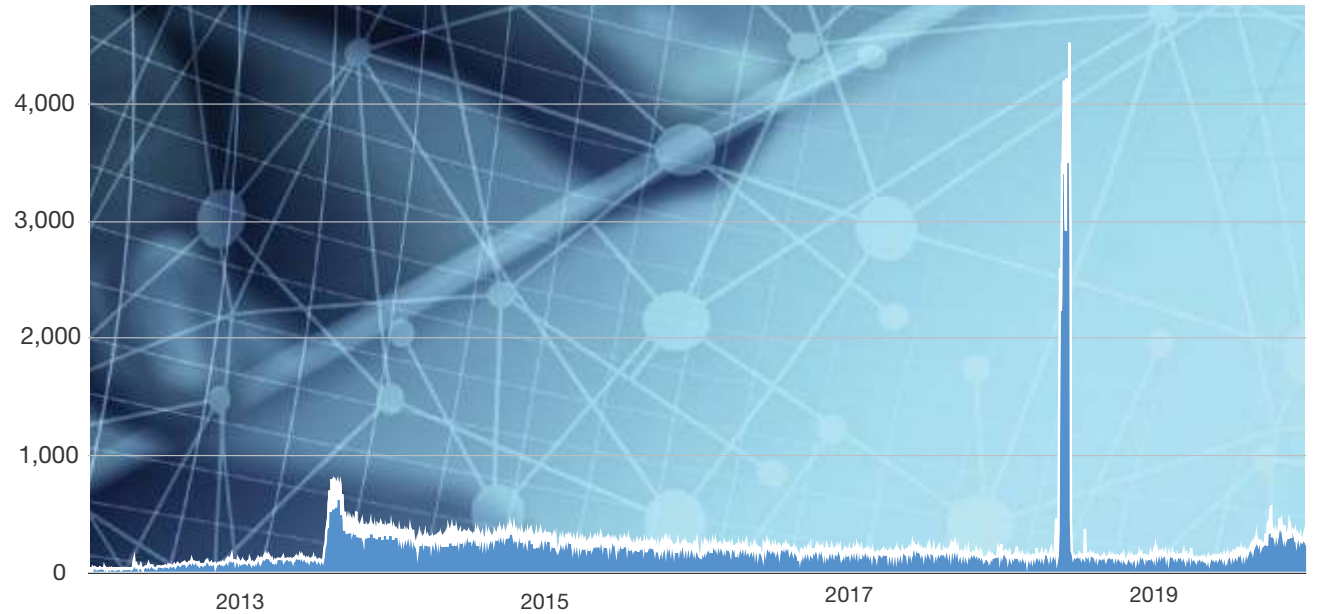


Tor Project - https://metrics.torproject.org/

4. CHDCND Lào

Lào có dân số khoảng 7,2 triệu[62]. Số liệu Tor (*Hình A4*) cho thấy việc sử dụng mạng Tor phần lớn vẫn ổn định từ năm 2015 đến năm 2020 ở mức trung bình khoảng 250 người dùng, với mức tăng nhẹ lên mức trung bình 500 người dùng kể từ đầu năm 2020.

Hình A4. Người dùng Tor được kết nối trực tiếp từ CHDCND Lào (tháng 1 năm 2012 đến tháng 7 năm 2020).



Tor Project - https://metrics.torproject.org/

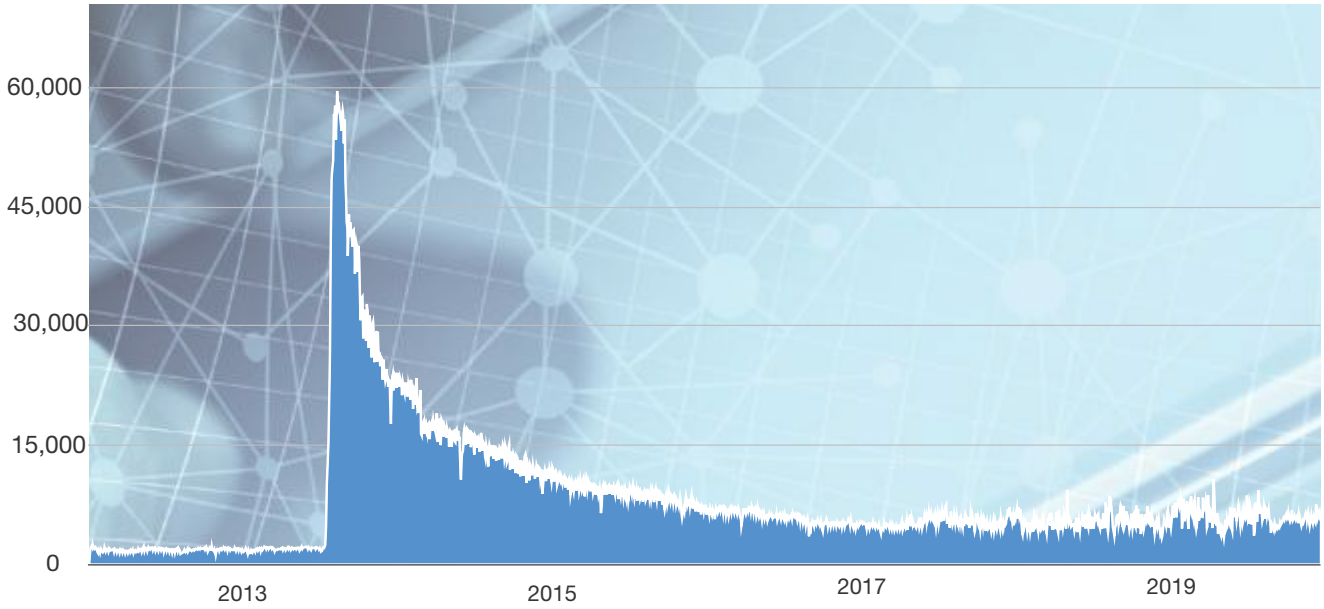
Tương tự như các quốc gia khác, cuối năm 2018 đã chứng kiến sự gia tăng lớn về số lượng người dùng cầu nối mạng Tor. Gần đây, đã có sự sụt giảm từ mức trung bình 400 người dùng xuống mức trung bình 25 người dùng.

Không có hoạt động nào được báo cáo từ Lào trên darknet I2P từ tháng 1 năm 2019 đến tháng 7 năm 2020.

5. Malaysia

Malaysia có dân số khoảng 32,4 triệu[63]. Số liệu Tor (*Hình A5*) cho thấy số lượng người dùng tăng mạnh trong năm 2013.Số lượng người dùng trung bình đã giảm từ năm 2013 đến năm 2017 và sau đó trung bình khoảng 5.000 người dùng mỗi ngày từ năm 2017 đến năm 2020.

Hình A5. Người dùng Tor được kết nối trực tiếp từ Malaysia (tháng 1 năm 2012 đến tháng 7 năm 2020).



Tor Project - https://metrics.torproject.org/

Mặc dù các kết nối trực tiếp của mạng Tor giảm, nhưng có sự gia tăng các kết nối cầu nối mạng Tor. Các kết nối cầu nối ở mức cao nhất khoảng 800 người dùng mỗi ngày vào giữa năm 2018. Từ năm 2019 đến năm 2020, người dùng cầu nối trung bình vẫn ổn định ở mức trung bình khoảng 150 người dùng.

Malaysia duy trì trung bình khoảng 85 người dùng mỗi ngày trên mạng I2P từ tháng 1 năm 2019 đến tháng 7 năm 2020. Số lượng người dùng dường như đã tăng gần gấp đôi kể từ tháng 1 năm 2020 từ khoảng 60 lên khoảng 100 người dùng.

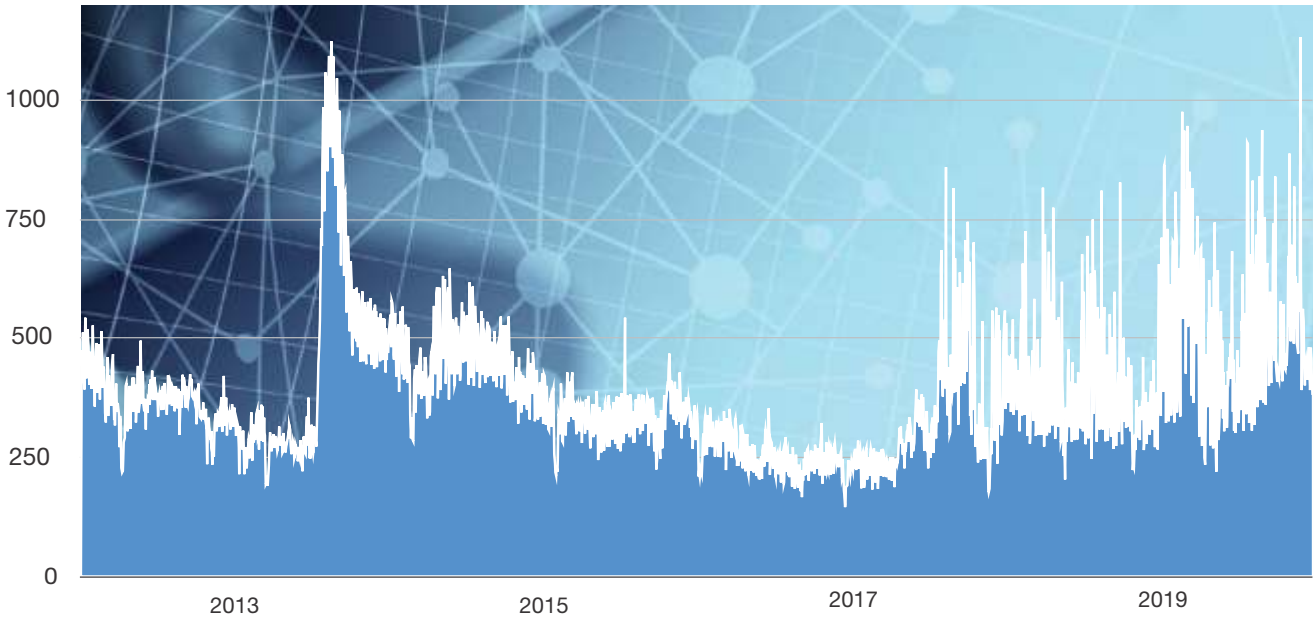
6. Myanmar

Myanmar có dân số khoảng 54,5 triệu[64]. Số liệu Tor (Hình A6) cho thấy số lượng người dùng tăng mạnh vào giữa năm 2013, giảm dần cho đến giữa năm 2017. Từ năm 2017, lượng người dùng trung bình đã tăng nhẹ, từ khoảng 200 người mỗi ngày lên khoảng 400 người vào năm 2020.

Như các quốc gia khác, đã có sự gia tăng lớn về người dùng cầu nối mạng Tor từ giữa năm 2018. Kể từ đó, lượng người dùng cầu nối mạng Tor đã giảm từ mức trung bình 500 người xuống mức trung bình 15 người dùng.

Không có hoạt động nào được báo cáo từ Myanmar trên darknet I2P từ tháng 1 năm 2019 đến tháng 7 năm 2020.

Hình A6. Người dùng Tor được kết nối trực tiếp từ Myanmar (tháng 1 năm 2012 đến tháng 7 năm 2020).



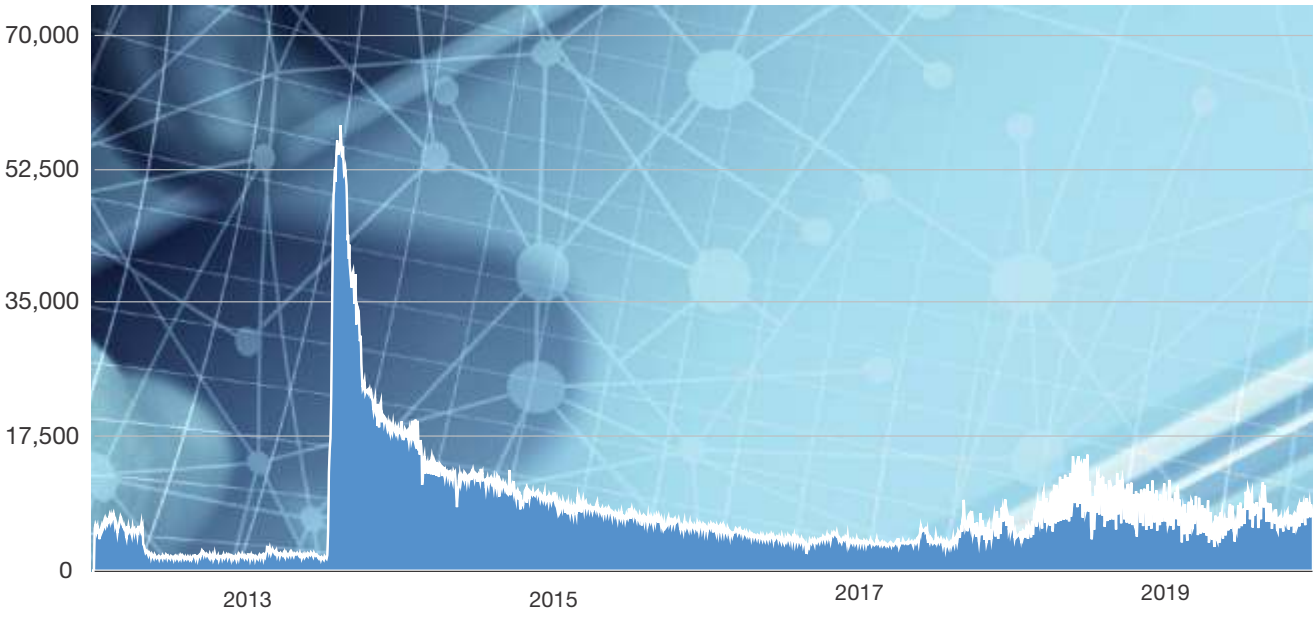
Tor Project - https://metrics.torproject.org/

7. Philippines

Philippines có dân số khoảng 109,9 triệu[65]. Số liệu Tor (*Hình A7*) cho thấy số lượng người dùng tăng mạnh vào giữa năm 2013 và sau đó giảm cho đến năm 2017. Từ năm 2017, chúng tôi chứng kiến số lượng người dùng tăng trung bình từ 5.000 lên khoảng 10.000 người dùng.

Tương tự như các quốc gia khác, giữa năm 2018 đã chứng kiến sự gia tăng lớn về số lượng người dùng cầu nối mạng Tor. Kể từ đó, lượng người dùng cầu nối mạng Tor đã giảm từ mức trung bình 3.500 người xuống mức trung bình 250 người dùng. Từ năm 2019 đến tháng 7 năm 2020, Philippines có trung bình 60 người dùng mạng I2P với phạm vi từ 30 đến 90 người dùng trong thời gian đó.

Hình A7. Người dùng Tor được kết nối trực tiếp từ Philippines (tháng 1 năm 2012 đến tháng 7 năm 2020).



Tor Project - https://metrics.torproject.org/

8. Singapore

Singapore có dân số khoảng 5,8 triệu[66]. Số liệu Tor (*Hình A8*) cho thấy sự gia tăng khá ổn định về người dùng mạng Tor trung bình từ năm 2013, với lượng người dùng trung bình tăng từ 5.000 lên 15.000 vào tháng 7 năm 2020.

Hình A8. Người dùng Tor được kết nối trực tiếp từ Singapore (tháng 1 năm 2012 đến tháng 7 năm 2020).

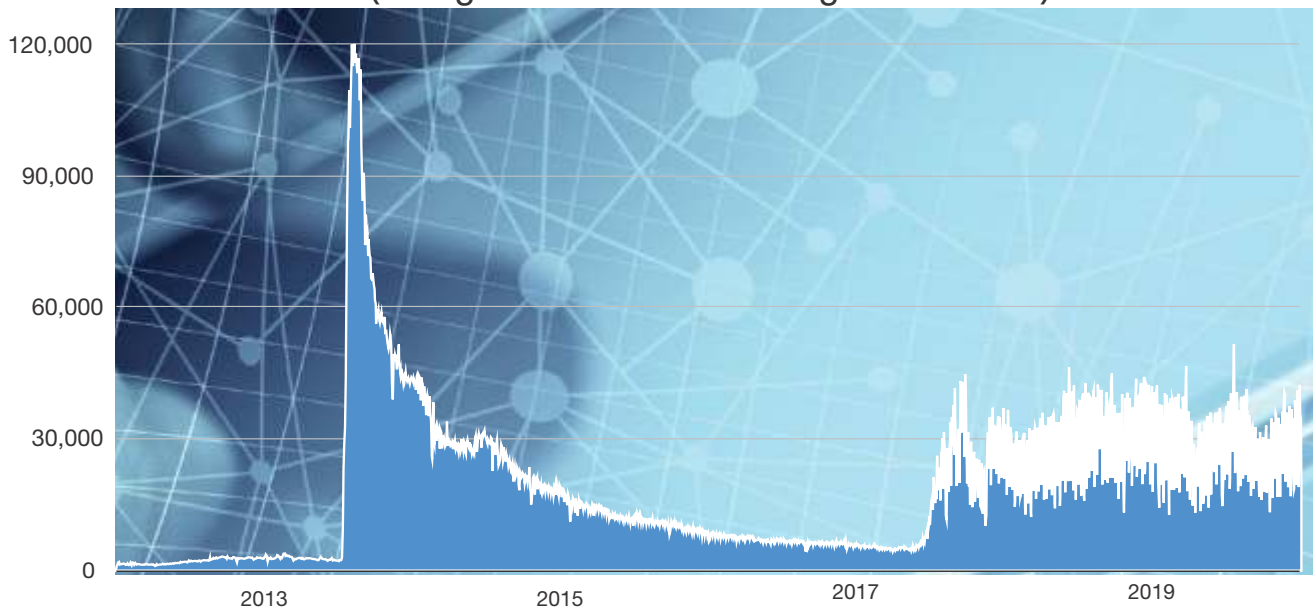
Tor Project - https://metrics.torproject.org/

Tương tự như những người dùng được kết nối trực tiếp, đã có sự gia tăng ổn định về người dùng cầu nối mạng Tor từ năm 2014 đến 2020, với trung bình khoảng 200 người dùng cầu nối mạng Tor vào tháng 7 năm 2020.

Từ năm 2019 đến tháng 7 năm 2020, Singapore đã tăng số lượng người dùng I2P từ 80 người mỗi ngày lên 140 người.Một lần tăng diễn ra vào tháng 11 năm 2019 và có một mức tăng ổn định khác kể từ tháng 1 năm 2020.

9. Thái Lan

Hình A9. Người dùng Tor được kết nối trực tiếp từ Thái Lan (tháng 1 năm 2012 đến tháng 7 năm 2020).



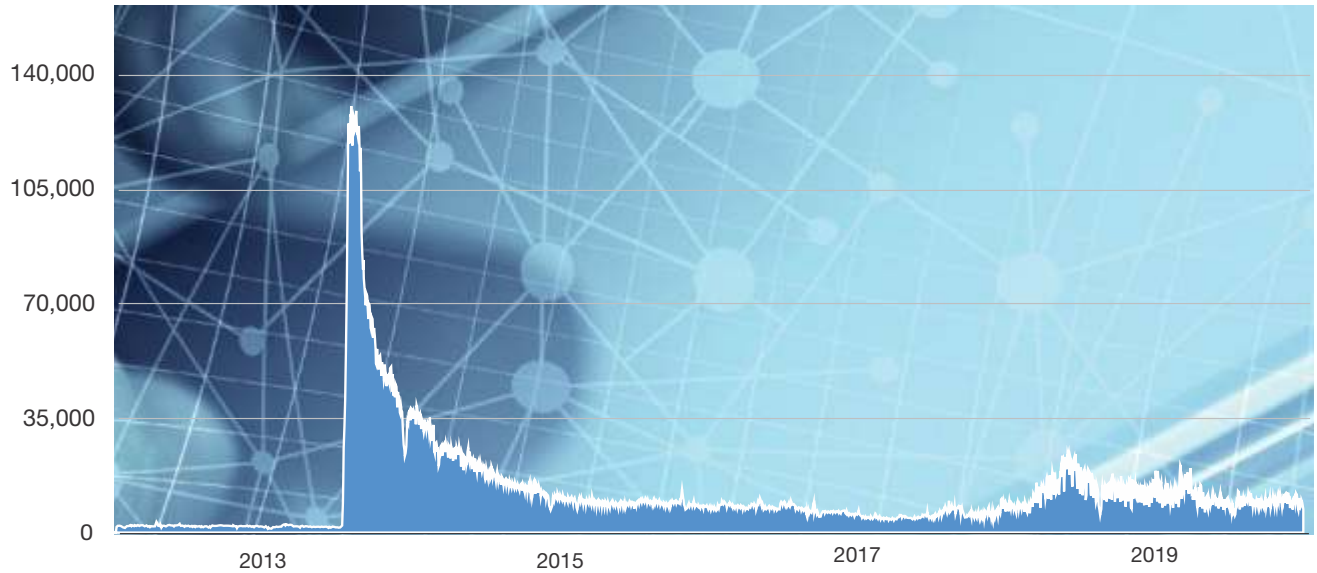
Tor Project - https://metrics.torproject.org/

Thái Lan có dân số khoảng 69,8 triệu[67]. Số liệu Tor (*Hình A9*) cho thấy lượng người dùng tăng mạnh vào giữa năm 2013 và giảm dần cho đến cuối năm 2017. Năm 2018, chúng tôi chứng kiến sự tăng số lượng người dùng lên khoảng 25.000 người và tiếp tục tăng nhẹ vào năm 2020. Người dùng cầu nối mạng Tor đạt mức cao nhất vào giữa năm 2018 với mức trung bình khoảng 4.000 người dùng mỗi ngày. Người dùng cầu nối giảm cho đến khi đạt mức trung bình khoảng 250 người dùng vào giữa năm 2020. Từ năm 2019 đến tháng 7 năm 2020, trung bình Thái Lan có 65 người dùng I2P. Người dùng dao động từ khoảng 30 đến 100 người với số lượng người dùng mạng I2P trung bình tăng từ đầu năm 2020.

10. Việt Nam

Việt Nam có dân số khoảng 97,5 triệu[68]. Số liệu Tor (*Hình A10*) cho thấy số lượng người dùng tăng mạnh vào giữa năm 2013 và sau đó giảm cho đến năm 2017. Số lượng người dùng trung bình tăng từ khoảng 6.000 người dùng vào năm 2017 lên khoảng 12.000 người dùng vào giữa năm 2020.

Hình A10. Người dùng Tor được kết nối trực tiếp từ Việt Nam (tháng 1 năm 2012 đến tháng 7 năm 2020).



Tor Project - https://metrics.torproject.org/

Người dùng cầu nối mạng Tor đạt mức cao nhất vào giữa năm 2018 với mức trung bình khoảng 15.000 người dùng mỗi ngày. Sau đó, người dùng cầu nối giảm cho đến khi đạt mức trung bình khoảng 250 người dùng vào giữa năm 2020.

Từ năm 2019 đến tháng 7 năm 2020, người dùng I2P đã giảm từ mức trung bình khoảng 200 người xuống mức trung bình khoảng 30 người vào giữa năm 2020.

A2: Phân tích kỹ thuật Darkweb

Dữ liệu Darkweb, bao gồm dữ liệu từ năm 2015–2020 đã được phân tích cho báo cáo này. Quá trình phân tích này đã tạo ra khoảng 200 triệu trang dữ liệu Darkweb bao gồm các trang web, nền tảng rò rỉ thông tin, thị trường, diễn đàn thảo luận, nhóm lợi ích và các vi phạm dữ liệu đã công bố. Dữ liệu được thu thập bằng cách sử dụng trình thu thập thông tin theo các liên kết và lưu trữ tất cả thông tin được thu thập. Các trang web Darkweb, đặc biệt là các marketplace và diễn đàn thảo luận, cần phải vượt qua nhiều trở ngại khác nhau, như CAPTCHA, tường phí, phát hiện hành vi theo kịch bản và xác minh.

Quá trình thu thập dữ liệu liên quan đến việc thu thập dữ liệu các trang web Onion bên trong mạng Tor và I2P.

Một hệ thống thu hoạch Darkweb cần có[69]:

1. Thu thập liên kết onion từ Deepweb và Darkweb,
2. Một hệ thống proxy nơi một số máy khách Tor được kết nối với mạng Tor,
3. Trình thu thập thông tin và công cụ tìm kiếm truy cập nội dung web HTTP có sẵn trên mạng Tor,
4. Logic để bỏ qua xác thực và phát hiện robot,
5. Phát hiện thông tin trùng lặp,
6. Trích xuất thông tin văn bản từ các tài liệu,
7. Lưu dữ liệu văn bản vào chỉ mục.

Hệ thống thu thập dữ liệu tự động thực hiện thu thập liên kết từ nội dung mà nó tìm thấy và quá trình thu thập thông tin liên tục theo các liên kết mới. Hơn nữa, có một chu kỳ để kiểm tra lại các địa chỉ URL được thu thập thông tin trong trường hợp có nội dung mới.

Hệ thống proxy là một tập hợp các máy khách phần mềm Tor và proxy cân bằng tải HTTP chọn một máy khách Tor cho mỗi tên miền onion.

Một số nội dung chỉ có sẵn sau khi đăng nhập và phát hiện robot (CAPTCHA). Nếu nội dung này được thu thập, cần có một hệ thống bỏ qua riêng, hệ thống này có thể đăng nhập và giải đáp các câu hỏi phát hiện robot.

A3:Kết quả phân tích kỹ thuật

Sau khi thu thập dữ liệu web để trích xuất và chuyển đổi dữ liệu không có cấu trúc từ Darkweb, dữ liệu có cấu trúc này đã được lưu trữ trên cơ sở dữ liệu[70]. Trong bước này, các kết nối và hành vi đã được nghiên cứu[71,72]. Việc khai thác dữ liệu xác định thông tin có thể được đính kèm hoặc liên kết với một quốc gia cụ thể hoặc với một tổ chức cư trú tại quốc gia cụ thể đó. Có hai mã nhận dạng: mã nhận dạng dành riêng cho quốc gia và mã nhận dạng dành riêng cho tổ chức.

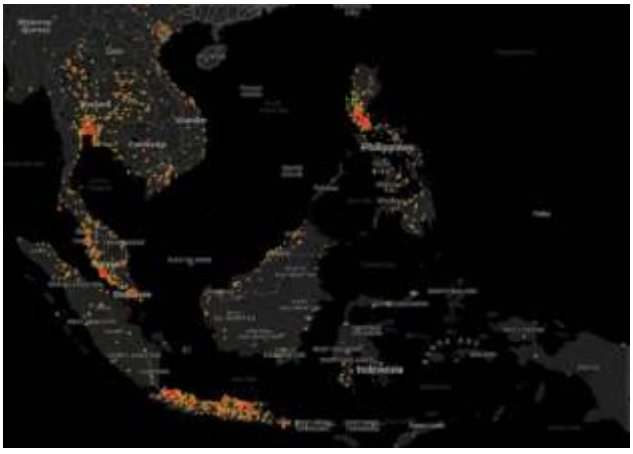
Mã nhận dạng dành riêng cho quốc gia:

1. Địa chỉ IP
2. Tên miền
3. Các tên thông dụng nhất của mỗi quốc gia
4. Số điện thoại có mã quốc gia
5. Số an ninh xã hội
6. Ngôn ngữ
7. Tọa độ GPS từ siêu dữ liệu hình ảnh

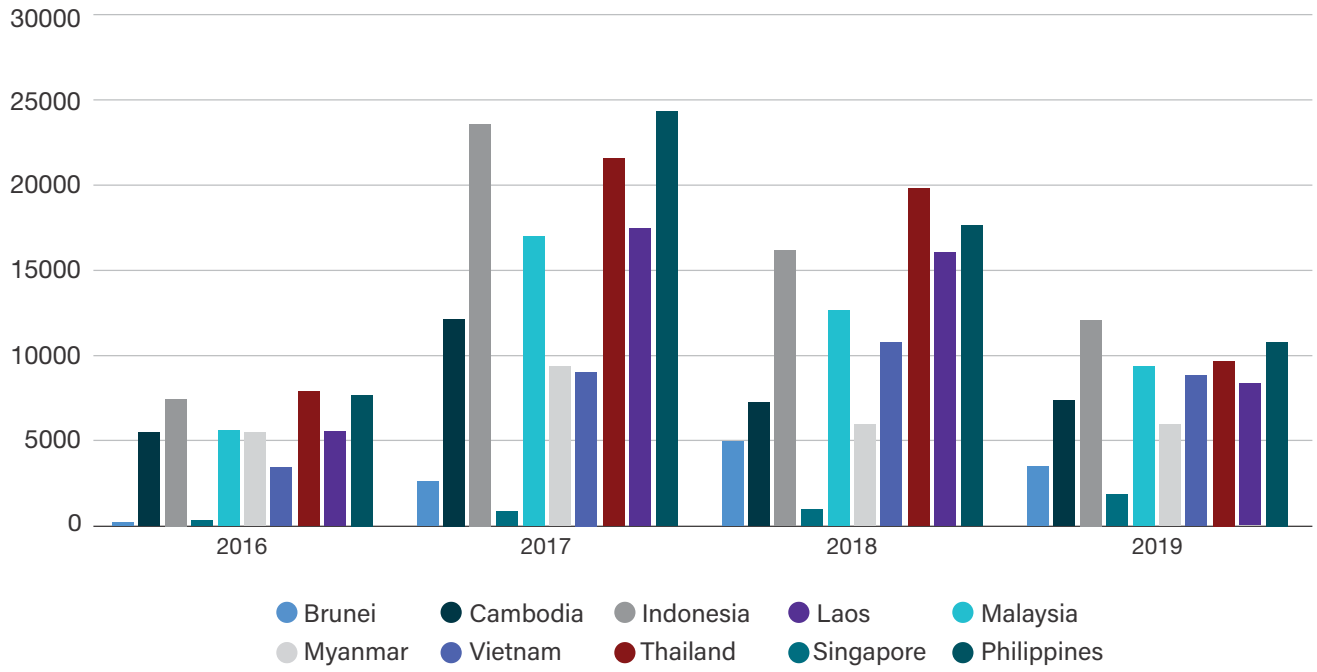
Mã nhận dạng dành riêng cho tổ chức

1. Tiết lộ thông tin nhạy cảm
2. Thảo luận
3. Hoạt động của marketplace4.Thông tin tài chính
5. Thông tin đăng nhập bị tiết lộ (mật khẩu)
6. Thông tin nhận dạng cá nhân
7. Nhắm mục tiêu theo nhóm hacker
8. Các cuộc tấn công và các thỏa hiệp trước đó.

Hình A11. Các địa chỉ IP được ánh xạ được đề cập trong mạng Tor từ Đông Nam Á.



Hình A12. Các quốc gia được đề cập trong các diễn đàn thảo luận trên Darkweb.



Giống như địa chỉ IP, số điện thoại nằm trên Darkweb trong nhiều trường hợp có liên quan đến nạn nhân của hoạt động phạm tội. Những số điện thoại này rất có thể là của nạn nhân của các vụ vi phạm dữ liệu và thường bị bọn tội phạm sử dụng cho các mục đích bất chính.

Nhìn chung, ngôn ngữ, số điện thoại, số ID quốc gia, v.v., có thể cung cấp một số thông tin về một vị trí. Darkweb đã được tìm kiếm bất kỳ mã nhận dạng dành riêng cho quốc gia nào. Các mã nhận dạng dành riêng cho quốc gia này thường xuất hiện trong các cuộc thảo luận trên diễn đàn, rò rỉ cơ sở dữ liệu và các thông tin khác được đăng trên Darkweb. Do đó, phần lớn dữ liệu theo vị trí cụ thể là dữ liệu về nạn nhân bị rò rỉ từ các quốc gia cụ thể. *Bảng A1* cho thấy một số mã nhận dạng có liên quan được tìm thấy trên Darkweb được liệt kê theo quốc gia. Mặc dù loại đánh giá này không cho phép đưa ra các giả thuyết, suy luận hoặc giả định về tội phạm/nạn nhân liên quan đến Darkweb, nhưng nó có thể sẽ hữu ích như một chỉ báo chung về số lượng hoạt động liên quan đến Darkweb mà một quốc gia đang phải đối mặt.

Indonesia là nước có số ID quốc gia bị rò rỉ nhiều nhất trên các diễn đàn. Giả sử đây là sự thật, điều đó cho thấy rằng có rất nhiều nạn nhân của các vụ vi phạm dữ liệu trong nước. Thông tin đó có thể được sử dụng để lừa đảo, lừa gạt hoặc tấn công nạn nhân, gia đình của họ hoặc các tổ chức liên quan. Tuy nhiên, dữ liệu này có thể được Chính phủ Indonesia sử dụng để tạo ra một chiến lược ứng phó với sự cố và giảm thiểu rủi ro.

Một số hình ảnh được chia sẻ trên Darkweb chứa siêu dữ liệu hình ảnh với các vị trí GPS (như vị trí bức ảnh được chụp). Thông thường, người dùng và các dịch vụ web sẽ xóa thông tin này. Tuy nhiên, một số hình ảnh vẫn chứa thông tin vị trí này và *Hình A13* cho thấy những hình ảnh này được chụp ở đâu tại Đông Nam Á. Điều này có thể sẽ tiết lộ các địa điểm liên quan đến hoạt động tội phạm có liên quan.

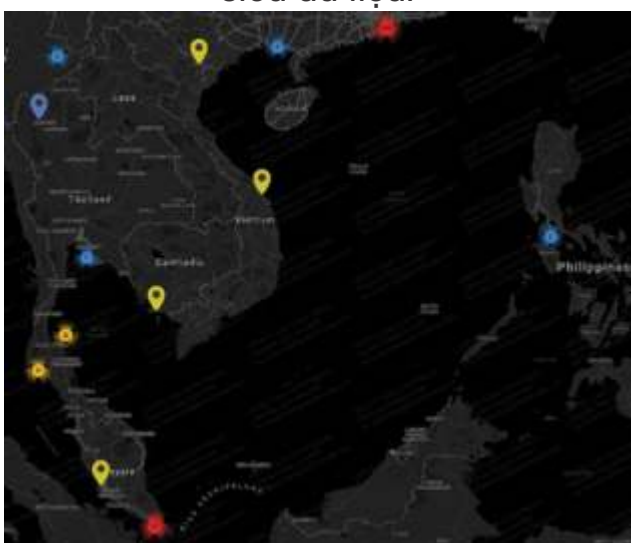
Bảng A1. Số lượng mã nhận dạng dữ liệu nhạy cảm được tìm thấy trên Darkweb được liệt kê theo quốc gia.

	Cambodia	Indonesia	Vietnam	Thailand	Philippines	Malaysia	Singapore	Laos	Brunei	Myanmar
Ngôn ngữ			21439	7945	15714					
điện thoại	18391	11685	7480	8022	907	581	582	4	10	60
Số ID Quốc gia		16073				47	571			
Các mặt hàng trên thị trường của quốc gia được đề cập	2198600	2232779	814943	2222729	2213301	2215632	2224558	784133	2189850	1444910
Địa chỉ IPv4	5832	94390	43657	55458	21143	50481	135631	3526	1586	4062
Tên miền	4339	128202	44681	86079	98837	113120	75261	218173	1723	4870
Quốc gia được đề cập trong bối cảnh CSE	16506	417	661	5139	968	167	19281	125	4	105
Quốc gia được đề cập trong diễn đàn	32382	59669	32199	59311	60812	44790	47929	3934	11323	25396

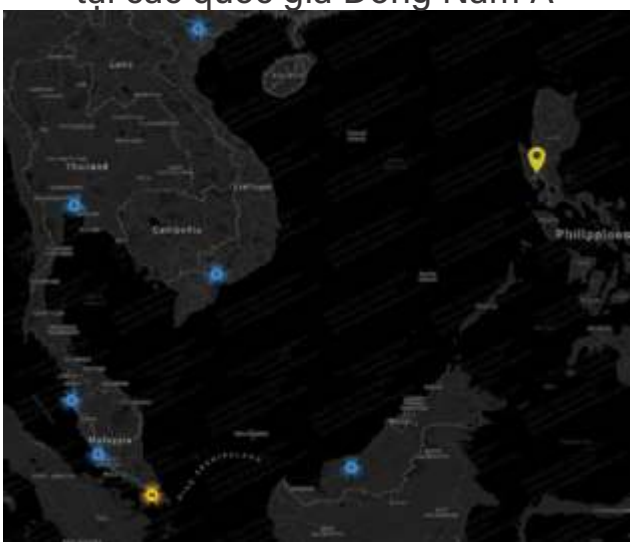
Mạng Tor là một mạng lớp phủ tự nguyện (một mạng xếp chồng lên nhau), bao gồm hơn 7.000 thiết bị chuyển tiếp. Người vận hành thiết bị chuyển tiếp mạng Tor không nhất thiết phải chịu trách nhiệm về lưu lượng đi qua thiết bị chuyển tiếp. Ở hầu hết các quốc gia, việc lắp đặt một thiết bị chuyển tiếp mạng Tor tự nguyện là hoàn toàn hợp pháp. Bất kỳ ai cũng có thể thao tác một nút bằng cách cài đặt phần mềm Tor ở chế độ bộ định tuyến và bắt đầu định tuyến lưu lượng truy cập mạng Tor qua máy chủ.

Như trong *Hình A14*, có tổng cộng 106 thiết bị chuyển tiếp Tor ở các nước Đông Nam Á (9 ở Indonesia, 12 ở Malaysia, 1 ở Philippines, 69 ở Singapore, 6 ở Thái Lan và 9 ở Việt Nam). Dữ liệu cho thấy Singapore là một địa điểm hấp dẫn để vận hành các thiết bị chuyển tiếp này.Điều này có lẽ là do các máy ảo giá rẻ để vận hành thiết bị chuyển tiếp có thể dễ dàng truy cập và cơ sở hạ tầng Internet đã phát triển tốt.

Hình A13. Vị trí chụp ảnh vẫn chứa siêu dữ liệu.

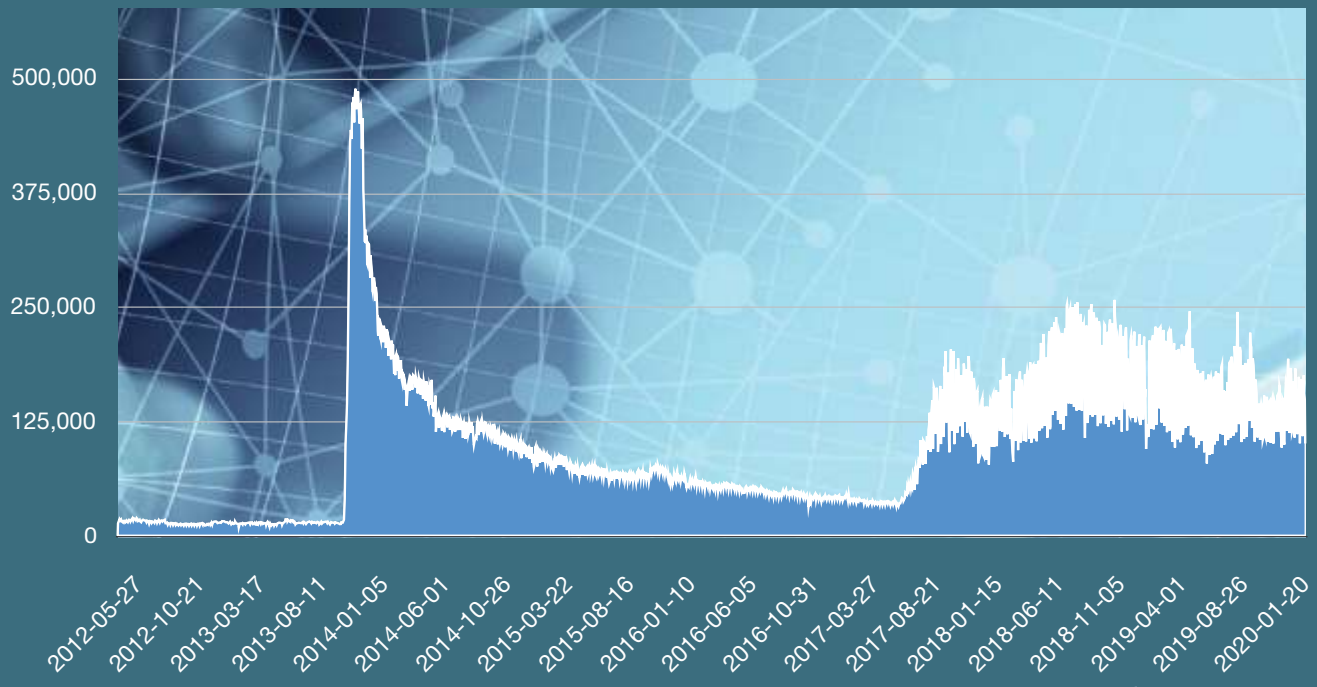


Hình A14. Các thiết bị chuyển tiếp Tor tại các quốc gia Đông Nam Á



Hình A15 cho thấy sự gia tăng tổng thể về mức độ phổ biến của mạng Tor ở các nước Đông Nam Á kể từ năm 2017, mặc dù lý do cho việc này không rõ ràng.

Hình A15. Người dùng Đông Nam Á được kết nối với mạng Tor (tháng 5 năm 2012 đến tháng 6 năm 2020).



Bảng thuật ngữ

Thuật ngữ		Định nghĩa
Mạng chia sẻ tệp ẩn danh		Mạng cho phép chia sẻ tệp và dữ liệu khác giữa những người dùng mạng. Chúng được thiết kế để gây khó khăn cho việc theo dõi nguồn gốc của cả người gửi và người nhận. Chúng thường là mạng Đồng cấp (P2P) với chức năng ẩn danh. Tuy nhiên, vẫn có thể thực hiện các chức năng chia sẻ tập trung với sự hỗ trợ của các mạng lớp phủ ẩn danh bổ sung, như Tor.
Trình duyệt web ẩn danh		Duyệt web ẩn danh cho phép người dùng truy cập các trang web mà không cho phép bất kỳ ai thu thập thông tin về những trang web mà người dùng đã truy cập.Các công cụ ẩn danh cố gắng ngăn chặn trình duyệt web lấy dấu vân tay và ẩn địa chỉ IP của khách truy cập. Các dịch vụ này thường sử dụng máy chủ proxy để xử lý từng yêu cầu HTTP.Khi người dùng yêu cầu một trang web bằng cách nhấp vào siêu liên kết hoặc nhập URL vào trình duyệt của họ, dịch vụ sẽ truy xuất và hiển thị thông tin bằng cách sử dụng máy chủ mà nó kiểm soát.Máy chủ từ xa (nơi có trang web được yêu cầu) nhận thông tin về dịch vụ lướt web ẩn danh thay cho thông tin của người dùng. Nguồn: https://www.lawweb.in/2012/10/use-of-annonymizer-for-better-privacy.html
APT	Tấn công có chủ đích	Như tên gọi 'có chủ đích' cho thấy một cuộc tấn công có chủ đích (APT) sử dụng các kỹ thuật tấn công liên tục, bí mật và tinh vi để chiếm và giữ quyền truy cập vào hệ thống trong một thời gian dài, với những hậu quả tiêu cực. Do cần nhiều nỗ lực để thực hiện một cuộc tấn công như vậy, APT thường được phân cấp ở các mục tiêu có giá trị cao, như các quốc gia và tập đoàn lớn, với mục đích cuối cùng là đánh cắp thông tin trong một thời gian dài, thay vì chỉ là 'tiếp cận' và rời đi nhanh chóng, như nhiều hacker mũ đen làm trong các cuộc tấn công mạng cấp thấp hơn. Nguồn: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats
Diễn đàn không đồng bộ		Một môi trường giao tiếp điện tử dựa trên Internet, cho phép người dùng đăng thông báo cho một số hoặc tất cả các thành viên xem. Thông báo vẫn được đăng cho đến khi người điều hành diễn đàn xóa bỏ thông báo. Không đồng bộ đề cập đến bản chất tĩnh của môi trường.Các bài đăng được thực hiện lần lượt, ẩn danh hoặc không và cung cấp hồ sơ điện tử bằng văn bản về các giao tiếp được thực hiện. Nguồn: https://www.igi-global.com/dictionary/peer-learning-social-interactions-asynchronous/1688
Băng thông		Băng thông là lượng truyền dữ liệu (Tốc độ) từ thiết bị này sang thiết bị khác trên mạng (bao gồm cả Internet). Nguồn: https://www.lifewire.com/what-is-bandwidth-2625809

Thuật ngữ		Định nghĩa
Botnet		'Botnet' (một thuật ngữ bắt nguồn từ các từ 'robot' và 'mạng') bao gồm một mạng lưới các máy tính được kết nối với nhau, được điều khiển từ xa thường bị nhiễm phần mềm độc hại, biến các hệ thống bị nhiễm thành cái gọi là 'bot', 'robot' hoặc 'zombies'. Nguồn: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
CaaS	Mô hình tội phạm như một dịch vụ	Mô hình kinh doanh Tội phạm như một Dịch vụ (CaaS) được sử dụng khi một nhóm tội phạm cung cấp một số hoặc tất cả các phần của hành động tội phạm như một dịch vụ cho các nhóm tội phạm khác. Điều này cho phép các nhóm tội phạm chuyên sâu vào các khía cạnh phạm tội cụ thể trong khi vẫn thu được lợi ích từ hành vi phạm tội tổng thể (thường có ít rủi ro hơn). CaaS bao gồm một loạt các dịch vụ thương mại tạo điều kiện cho hầu hết mọi loại tội phạm mạng. Tội phạm có thể tự do mua các dịch vụ đó, như cho thuê mạng botnet, tấn công từ chối dịch vụ, phát triển phần mềm độc hại, đánh cắp dữ liệu và bẻ khóa mật khẩu, để tự thực hiện hành vi phạm tội. Nguồn: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014
CAPTCHA	Phép thử Tự động để Phân biệt Máy tính và Con người	CAPTCHA là một phương pháp được sử dụng để bảo vệ các trang web chống thư rác. Mục đích là ngăn các trang web tương tác bị spam bằng cách lọc ra thông tin đầu vào được tạo tự động. Nguồn: https://www.ionos.com/digitalguide/online-marketing/online-sales/captcha-codes-and-images-for-spam-protection/
Tránh kiểm duyệt		Tránh kiểm duyệt Internet là việc sử dụng các phương pháp và công cụ khác nhau để vượt qua kiểm duyệt Internet. Ví dụ, kiểm duyệt Internet có thể giám sát và chặn một số yêu cầu trang web nhất định. Tránh kiểm duyệt có thể cố gắng che giấu hoặc làm xáo trộn yêu cầu, hoặc qua mặt người giám sát bằng cách ẩn yêu cầu thông qua một máy tính không được kiểm duyệt. Nguồn: https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship
Clearnet		Clearnet là mạng Internet 'thông thường', có thể được khám phá bằng cách sử dụng các kỹ thuật truy vấn DNS và thu thập thông tin liên kết. Những kỹ thuật này được sử dụng bởi các công cụ tìm kiếm điển hình như Google, Bing và Yahoo. Đó là mạng Internet non-dark, non-Tor không được mã hóa. Nguồn: https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

Thuật ngữ		Định nghĩa
Tiền điện tử		Tiền điện tử là các token điện tử được tạo ra bởi các mạng máy tính để thay thế các loại tiền tệ truyền thống.Các token điện tử bằng tiền kỹ thuật số có giá trị dựa trên việc trao đổi tiền tệ thông thường và hàng hóa lấy token thông qua các sàn giao dịch Internet đặc biệt, như BitPay. Các sàn giao dịch này hoạt động giống như PayPal nhưng không liên kết với công ty đó. Nguồn: https://www.kaspersky.com/resource-center/definitions/what-is-bitcoin https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
CSE	Bóc lột Tình dục Trẻ em	Ngược đãi tình dục trẻ em bao gồm nhưng không giới hạn ở lạm dụng tình dục trẻ em, tấn công tình dục trẻ em, tài liệu lạm dụng tình dục trẻ em, tảo hôn hoặc ép buộc, cũng như sản xuất hình ảnh lạm dụng đó và chia sẻ những hình ảnh đó trực tuyến . Nguồn: https://www.icmec.org/resources/glossary/ https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
CSEM	Tài liệu về Bóc lột Tình dục Trẻ em	Tài liệu về Bóc lột Tình dục Trẻ em là bất kỳ tài liệu nào mô tả bằng hình ảnh một đứa trẻ thực hiện hành vi khiêu dâm thực tế hoặc mô phỏng. Trong đó cũng có thể bao gồm bất kỳ tài liệu nào thường mô tả một đứa trẻ về mặt tình dục. Nguồn: https://www.ecpat.org/what-we-do/online-child-sexual-exploitation/ https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
Tấn công mạng		Một cuộc tấn công mạng xảy ra khi tội phạm mạng cố gắng gây thiệt hại về danh tiếng hoặc gây tổn hại cho doanh nghiệp hoặc cá nhân, hoặc đánh cắp dữ liệu có giá trị. Các cuộc tấn công mạng có thể hướng tới các cá nhân, nhóm, tổ chức hoặc chính phủ. Nguồn: https://us.norton.com/Internetsecurity-emerging-threats-cyberattacks-on-the-rise-what-to-do.html
Trình trộn tiền điện tử		Dịch vụ trộn tiền điện tử là một dịch vụ được cung cấp để trộn các khoản tiền điện tử có khả năng nhận dạng với các khoản không liên quan khác, để che dấu cách truy xuất nguồn gốc khoản tiền. Nguồn: https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

Thuật ngữ		Định nghĩa
Darknet/ Darkweb		Một phần bảo mật tương đối của World Wide Web không được lập chỉ mục bởi các công cụ tìm kiếm và chỉ có thể được truy cập bằng phần mềm chuyên dụng như trình duyệt Tor. Nguồn: https://iaca-dark web-tools.com/dictionary/ Một mạng, được xây dựng trên mạng Internet, được ẩn có chủ đích; đã được thiết kế đặc biệt để ẩn danh. Không giống như Deepweb, darknet chỉ có thể truy cập được bằng các công cụ và phần mềm đặc biệt - các trình duyệt và giao thức khác ngoài liên kết trực tiếp hoặc thông tin đăng nhập. Nguồn: Europol, 2017 "Ma túy và darknet – quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
Vi phạm dữ liệu		Một hành vi vi phạm dữ liệu làm lộ thông tin bảo mật, nhạy cảm hoặc được bảo vệ cho một người không được phép biết. Dữ liệu trong một vụ vi phạm dữ liệu được xem và/hoặc chia sẻ khi chưa được phép. Nguồn: https://www.kaspersky.com/resource-center/definitions/data-breach
Deep web		Một phần của mạng Internet không được lập chỉ mục bởi các công cụ tìm kiếm. Deep web chứa những thứ như mạng nội bộ, thông tin ngân hàng, trang web thành viên, cũng như Darkweb. Cách duy nhất để truy cập Deep web là tiến hành tìm kiếm trong một trang web cụ thể. Ví dụ, cơ sở dữ liệu và thư viện của chính phủ chứa một lượng lớn dữ liệu Deep web. Nguồn: https://iaca-dark web-tools.com/dictionary/ Nguồn: Europol, 2017 "Ma túy và darknet – quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
DDoS	Tấn công Từ chối Dịch vụ Phân tán	Tấn công Từ chối Dịch vụ Phân tán cố gắng chặn người dùng hợp pháp truy cập vào một số dịch vụ bằng cách sử dụng một mạng lưới hệ thống phân tán để lấn át tài nguyên của mục tiêu. Nguồn: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Thuật ngữ		Định nghĩa
DoS	Tấn công Từ chối Dịch vụ	Tấn công Từ chối Dịch vụ cố gắng chặn người dùng hợp pháp truy cập vào một số dịch vụ. Ví dụ, bằng cách lấn át một trang web được nhắm mục tiêu đến mức làm sập nó hoặc khiến nó quá tải để có thể truy cập được. Tấn công Từ chối Dịch vụ thành công có thể làm tê liệt bất kỳ thực thể nào phụ thuộc vào sự hiện diện trực tuyến bằng cách làm cho trang web của họ gần như vô dụng. Nguồn: https://evestigate.com/cyber-crime-hacker-terms-to-know/
Doxing		Doxing là tìm kiếm và công bố thông tin cá nhân hoặc thông tin nhận dạng về một cá nhân hoặc bí danh của họ mà họ không biết hoặc không được phép. Nguồn: https://iaca-dark web-tools.com/dictionary/
Trang web thương mại điện tử		Các trang web cho phép các cá nhân mua và bán hàng hóa và dịch vụ trực tuyến.
Mã hóa		Quá trình chuyển đổi dữ liệu sang dạng không thể nhận dạng hoặc "được mã hóa". Nó thường được sử dụng để bảo vệ thông tin nhạy cảm, bao gồm tệp, thiết bị lưu trữ và truyền dữ liệu để chỉ các bên được ủy quyền mới có thể xem được. Nguồn: Europol, 2017 "Ma túy và darknet – quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
Hệ thống thanh toán ký quỹ		Hệ thống thanh toán của bên thứ ba, thường là một marketplace, giữ tiền trong khi thực hiện giao dịch giữa người mua và người bán. Nguồn: https://iaca-dark web-tools.com/dictionary/
Exit scam		Một hành vi lừa đảo trong đó quản trị viên thị trường darknet hoặc nhà cung cấp ngừng hoạt động trong khi đánh cắp càng nhiều tiền càng tốt từ người dùng và/hoặc người mua trong quá trình này. Nguồn: Europol, 2017 "Ma túy và darknet – quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

Thuật ngữ		Định nghĩa
Giả mạo		Hành động tạo ra một vật giả để nó có thể được chấp nhận là hàng thật. Nguồn: https://legal-dictionary.thefreedictionary.com/forgery Hành vi giả mạo thường yêu cầu hai yếu tố cần thiết: (i) thay đổi hoặc thao túng dữ liệu máy tính, và (ii) mục đích cụ thể để sử dụng dữ liệu như thể chúng là dữ liệu xác thực. Ngoài ra, các quốc gia có thể mở rộng định nghĩa về đối tượng giả mạo truyền thống. Ví dụ, một số quốc gia ở Châu Âu đã che đậy hành vi giả mạo liên quan đến máy tính bằng cách mở rộng định nghĩa 'tài liệu' để bao gồm dữ liệu máy tính. Các quốc gia khác áp dụng các quy định chung đối với hành vi giả mạo liên quan đến máy tính mà không sửa đổi luật nếu các quy định truyền thống về giả mạo có thể được hiểu là bao gồm các tài liệu, chữ ký và dữ liệu kỹ thuật số. Nguồn: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
Hacktivism		Hacktivism là việc cố ý truy cập vào các hệ thống, trang web và/hoặc dữ liệu mà không được phép hoặc vượt quá quyền truy cập được phép và/hoặc cố ý can thiệp vào hoạt động và/hoặc khả năng truy cập của hệ thống, trang web và dữ liệu mà không được phép hoặc vượt quá quyền truy cập được phép, để tạo ra sự thay đổi trong xã hội hoặc chính trị. Nguồn: Maras, Marie-Helen. (2016). Cybercriminology. Oxford University Press.
Dịch vụ ẩn		Một tính năng được mạng Tor cung cấp cho phép người dùng lưu trữ ẩn danh nội dung và dịch vụ trên Darkweb. Nguồn: Europol, 2017 "Ma túy và darknet - quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
HTTPS	Giao thức Truyền tải Siêu văn bản Bảo mật	Giao thức truyền tải này là ngôn ngữ mà máy khách web - thường là trình duyệt - và máy chủ web giao tiếp với nhau. HTTPS là phiên bản của giao thức truyền tải sử dụng giao tiếp được mã hóa. Nguồn: https://www.ionos.com/digitalguide/hosting/technical-matters/what-is-https/

Thuật ngữ		Định nghĩa
Trộm cắp danh tính - có liên quan đến máy tính		Đề cập đến các hành vi liên quan đến việc truyền tải, sở hữu hoặc sử dụng các phương tiện nhận dạng của người khác được lưu trữ trong dữ liệu máy tính mà không có quyền, với mục đích thực hiện, hỗ trợ hoặc tiếp tay cho bất kỳ hoạt động phạm tội bất hợp pháp nào.Ví dụ, đây là trường hợp nếu một kẻ phạm tội, không có quyền, lấy thông tin giấy phép lái xe từ một hệ thống máy tính và bán dữ liệu đó hoặc sử dụng nó để che giấu danh tính thật của mình khi phạm tội. Nguồn: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
I2P	Dự án Internet Vô hình	Phần mềm cung cấp quyền truy cập vào mạng cho phép trình duyệt web, nhắn tin và truyền tệp ẩn danh. Nguồn: https://iaca-dark web-tools.com/dictionary/ Một giải pháp thay thế cho các dịch vụ ẩn Tor. Đó là một mạng lớp phủ dựa trên việc truyền thông điệp giữa các bộ định tuyến bằng cách sử dụng định tuyến garlic với một bảng băm phân tán cho một thư mục chung của các bộ định tuyến có sẵn. Nguồn: Europol, 2017 "Ma túy và darknet - quan điểm cho nghiên cứu và chính sách thực thi" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
Địa chỉ IP	Địa chỉ giao thức Internet	Địa chỉ của thiết bị được kết nối trong mạng IP (mạng TCP/IP), là tiêu chuẩn toàn cầu cho cả kết nối mạng nội bộ và Internet. Mọi máy tính để bàn và máy tính xách tay, máy chủ, modem, bộ định tuyến, điện thoại thông minh, máy tính bảng và TV thông minh đều được gán một địa chỉ IP khi kết nối mạng. Mỗi gói IP truyền qua mạng IP đều chứa địa chỉ IP nguồn và địa chỉ IP đích. Nguồn: https://www.pcmag.com/encyclopedia/term/ip-address

Chỉ mục

1 https://www.unodc.org/unodc/en/frontpage/2019/June/world-drug-report-2019_-35-million-people-worldwide-suffer-from-drug-use-disorders-while-only-1-in-7-people-receive-treatment.html

2 Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/

3 Ibid.

4 D. Moore and T. Rid, "Cryptopolitik and the Darknet," Survival, vol. 58, no. 1, pp. 7–38, Jan. 2016, doi:10.1080/00396338.2016.1142085.

5 G. Owen and N. Savage, "The Tor Dark Net," 2015.

6 J. Nurmi, "Understanding the Usage of Anonymous Onion Services Empirical Experiments to Study Criminal Activities in the Tor Network," 2019.

7 J. Nurmi and M. S. Niemelä, "Tor de-anonymisation techniques," in 11th International Conference, NSS, 2017.

8 "Category:Anonymous file sharing networks - Wikipedia."[Online]. Available: https://en.wikipedia.org/wiki/Category:Anonymous_file_sharing_networks.[Accessed:07-Jan-2020].

9 K. Loesing, "Privacy-enhancing Technologies for Private Services," 2009.

10 K. S. Bauer, "Improving Security and Performance in Low Latency Anonymous Networks," 2011.

11 R. G. Jansen, "Privacy Preserving Performance Enhancements for Anonymous Communication Networks," 2012.

12 D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding Routing Information," in International Workshop on Information Hiding, 1996.

13 R. Dingledine, N. Mathewson, and P. Syverson, "Tor:The Second-Generation Onion Router," in Proceedings of the 13th USENIX Security Symposium, 2004.

14 https://www.torproject.org

15 Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/https://cyberintelligencehouse.com/

16 "Tor Metrics. "[Online]. Available: https://metrics.torproject.org

17 Ibid.

18 Ibid.

19 C. Dion-Schwarz, D. Manheim, and P. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. RAND Corporation, 2019.

20 K. Kruithof, J. Aldridge, D. Hétu, M. Sim, E. Dujso, and S. Hoorens, Internet-facilitated drugs trade:An analysis of the size, scope and the role of the Netherlands.RAND Corporation, 2016.

21 Ibid.

22 "AlphaBay, the Largest Online 'Dark Market,' Shut Down | OPA | Department of Justice." [Online]. Available: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down/. [Accessed:10-Mar2020].

23 "Dark web drug bust: Three arrested for Singapore connect | Cities News, The Indian Express." [Online]. Available: https://indianexpress.com/article/cities/delhi/dark-web-drug-bust-3-arrested-for-singapore-connect-6276649/ [Accessed: 10-Mar- 2020].

24 "Australian Peter Scully given life sentence for human trafficking, rape in Philippines, reports say - ABC News (Australian Broadcasting Corporation)." [Online]. Available: https://www.abc.net.au/news/2018-06-14/australian-peter-scully-convicted-in-philippines/9868958. [Accessed: 10-Mar-2020].

25 Ibid.

26 "Alleged pedophilia 'dark web' site bust by Interpol brings arrests in Thailand, US and Australia and rescue of 50 children today - CBS News." [Online]. Available: https://www.cbsnews.com/news/pedophilia-ring-dark-web-interpol-operation-blackwrist-thailand-us-australia-children-rescued/. [Accessed: 10-Mar-2020].

27 "Paedophile Richard Huckle 'murdered' in prison | UK news | The Guardian." [Online]. Available: https://www.theguardian.com/uk-news/2019/oct/14/paedophile-richard-huckle-found-dead-in-prison. [Accessed: 10-Mar-2020].

28 Ibid.

29 "US indicts Russian cybercrime Dark Web market 'Infraud Organization' suspect Sergey Medvedev, arrested in Thailand - CBS News. "[Online]. Available: https://www.cbsnews.com/news/us-russia-cybercrime-dark-web-market-suspect-sergey-medvedev-thailand. [Accessed: 10-Mar-2020].

30 Tor Metrics. https://metrics.torproject.org/

31 Roderic Broadhurst, Matthew Ball, Chuxuan Jessie Jiang. (2020) Availability of COVID-19 related products on Tor darknet markets. https://www.aic.gov.au/sites/default/files/2020-05/sb24_availability_of_covid-19_related_products_on_tor_darknet_markets.pdf

32 CISOMAG. (2020) Over 230K Indonesian COVID-19 Patients' Records Exposed on Darknet. https://cisomag.eccouncil.org/indonesian-patients-data-leak/

33 PWC. (2020) Why has there been an increase in cyber security incidents during COVID-19?. https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

34 Microsoft Threat Intelligence.(2020) Open-sourcing new COVID-19 threat intelligence. https://www.microsoft.com/security/blog/2020/05/14/open-sourcing-covid-threat-intelligence/

35 Dumrongkiat Mala. (2020) ‹Dark net› a godsend for paedophiles. https://www.bangkokpost.com/thailand/general/1860539/dark-net-a-godsend-for-paedophiles

36 Thomas Brewster. (2020) Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame?. https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/#15c5a0204c9c

37 Michael Kapilkov.(2020) Criminals Are Selling COVID-19 Infected Blood on the Darknet. https://cointelegraph.com/news/criminals-are-selling-covid-19-infected-blood-on-the-darknet

38 Ibid.

39 M. J. Barratt, "Silk Road: Ebay for drugs," Addiction, vol. 107, no. 3, pp. 683–683, Mar. 2012, doi:10.1111/j.1360-0443.2011.03709.x.

40 M. C. van Hout and T. Bingham, "'Surfing the Silk Road':A study of users' experiences," International Journal of Drug Policy, vol. 24, no. 6, pp. 524–529, Nov. 2013, doi:10.1016/j.drugpo.2013.08.011.

41 M. J. Barratt, "Silk Road: Ebay for drugs," Addiction, vol. 107, no. 3, pp. 683–683, Mar. 2012, doi:10.1111/j.1360-0443.2011.03709.x.

42 M. C. van Hout and T. Bingham, "'Surfing the Silk Road': A study of users' experiences," International Journal of Drug Policy, vol. 24, no. 6, pp. 524–529, Nov. 2013, doi: 10.1016/j.drugpo.2013.08.011.

43 N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," Proceedings of the 22nd international conference on World Wide Web, Jul. 2013.

44 J. Martin, "Lost on the Silk Road: Online drug distribution and the 'cryptomarket,'" Criminology & Criminal Justice, vol. 14, no. 3, pp. 351–367, Jul. 2014, doi:10.1177/1748895813505234.

45 J. Nurmi and M. S. Niemelä, "Tor de-anonymisation techniques," in 11th International Conference, NSS, 2017.

46 J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet As An Online Drug Market Innovation," 2015.

47 J. Nurmi, "Understanding the Usage of Anonymous Onion Services Empirical Experiments to Study Criminal Activities in the Tor Network," 2019.

48 J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet as an Online Drug Market Innovation," 2015.

49 K. Masson and A. Bancroft, "'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets," International Journal of Drug Policy, vol. 58, pp. 78–84, 2018.

50 G. Owen and N. Savage, "Empirical analysis of Tor hidden services," IET Information Security, vol. 10, no. 3, pp. 113–118, May 2016, doi: 10.1049/iet-ifs.2015.0121.

51 A. Biryukov, I. Pustogarov, and R. P. Weinmann, "Trawling for tor hidden services: Detection, measurement, deanonymization," in Proceedings - IEEE Symposium on Security and Privacy, 2013, pp. 80–94, doi: 10.1109/SP.2013.15.

52 J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet as an Online Drug Market Innovation," 2015.

53 K. Masson and A. Bancroft, "'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets," International Journal of Drug Policy, vol. 58, pp. 78–84, 2018.

54 "Payment Fraud | Crime areas | Europol." [Online]. Available: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud. [Accessed: 18-May-2020].

55 Ibid.

56 Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/

57 Dan Goodin. (2013) Sudden spike of Tor users likely caused by one "massive" botnet. Ars Technica. https://arstechnica.com/information-technology/2013/09/sudden-spike-of-tor-users-likely-caused-by-one-massive-botnet/

58 United Nations. (2019) World Population Prospects 2019. https://population.un.org/wpp/

59 Ibid.

60 Dan Goodin. (2013) Sudden spike of Tor users likely caused by one "massive" botnet. Ars Technica. https://arstechnica.com/information-technology/2013/09/sudden-spike-of-tor-users-likely-caused-by-one-massive-botnet/

61 United Nations. (2019) World Population Prospects 2019. https://population.un.org/wpp/

62 Ibid.

63 Ibid.

64 Ibid.

65 Ibid.

66 Ibid.

67 Ibid.

68 Ibid.

69 A. Biryukov, I. Pustogarov, and R. P. Weinmann, "Trawling for tor hidden services: Detection, measurement, deanonymization," in Proceedings - IEEE Symposium on Security and Privacy, 2013, pp. 80–94, doi:10.1109/SP.2013.15.

70 M. Wesam, A. Nabki, E. Fidalgo, E. Alegre, and I. de Paz, "Classifying Illegal Activities on Tor Network Based on Web Textual Contents," 2017.

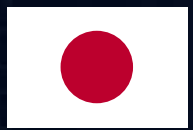
71 "Tor Metrics." [Online]. Available: https://metrics.torproject.org.

72 E. Çalışkan, T. Minárik, and A.-M. Osula, "Technical and Legal Overview of the Tor Anonymity Network Technical and Legal Overview of the Tor Anonymity Network," 2015.

Cơ quan Phòng chống Ma túy và
Tội phạm của Liên Hợp Quốc (UNODC)
Regional Office for Southeast Asia and
the Pacific
United Nations Building, 3rd floor, Block B
Rajadamnern Nok Avenue Bangkok
10200, Thailand
Website: https://www.unodc.org/
southeastasiaandpacific
Twitter: @UNODC SEAP

Global Programme on CybercrimeVienna
International Centre P.O.Box 500, A-1400
Vienna, Austria.
Website: https://www.unodc.org/unodc/
en/cybercrime/global-programme-
cybercrime.html
Twitter: @UN Cyber

UNODC xin chân thành cảm ơn
Chính phủ Nhật Bản đã tài trợ cho
nghiên cứu này.



UNODC
Cơ quan Phòng chống Ma túy và Tội phạm của Liên Hợp Quốc