CYBER SECURITY THREAT REPORT

# BÁO CÁO THƯỜNG NIÊN AN NINH MẠNG QUÝ I/2021

*Thống kê số liệu các cuộc tấn công mạng tại Việt Nam và trên thế giới trong quý I/2021*

VinaAspire®

## Giới thiệu

Báo cáo an ninh mạng là báo cáo định kỳ được thực hiện bởi Vina Aspire, nhằm đánh giá mức độ và xu hướng tấn công vào bảo mật thông tin trên thế giới và tại Việt Nam.

Báo cáo dưới đây tổng hợp số liệu tấn công mạng tại Việt Nam và trên thế giới trong thời gian: 1/1 - 10/4/2021

## Tuyên bố miễn trừ trách nhiệm

Do giới hạn của công nghệ và kỹ thuật, những số liệu được công bố trong báo cáo này chỉ mang tính chất tham khảo. Vina Aspire không chịu trách nhiệm với bất kỳ số liệu hoặc thông tin nào trong báo cáo này.

Trừ khi chúng tôi đưa ra sự đồng ý trước bằng văn bản rõ ràng, không một phần nào của báo cáo này được phép sao chép, phân phối, truyền đạt cho bên thứ ba nào.

Chúng tôi không chịu bất kì trách nhiệm pháp lý nào nếu báo cáo này được sử dụng trái với mục đích ban đầu, cũng như bất kỳ bên thứ ba nào liên quan đến báo cáo này.

# TIÊU ĐIỂM

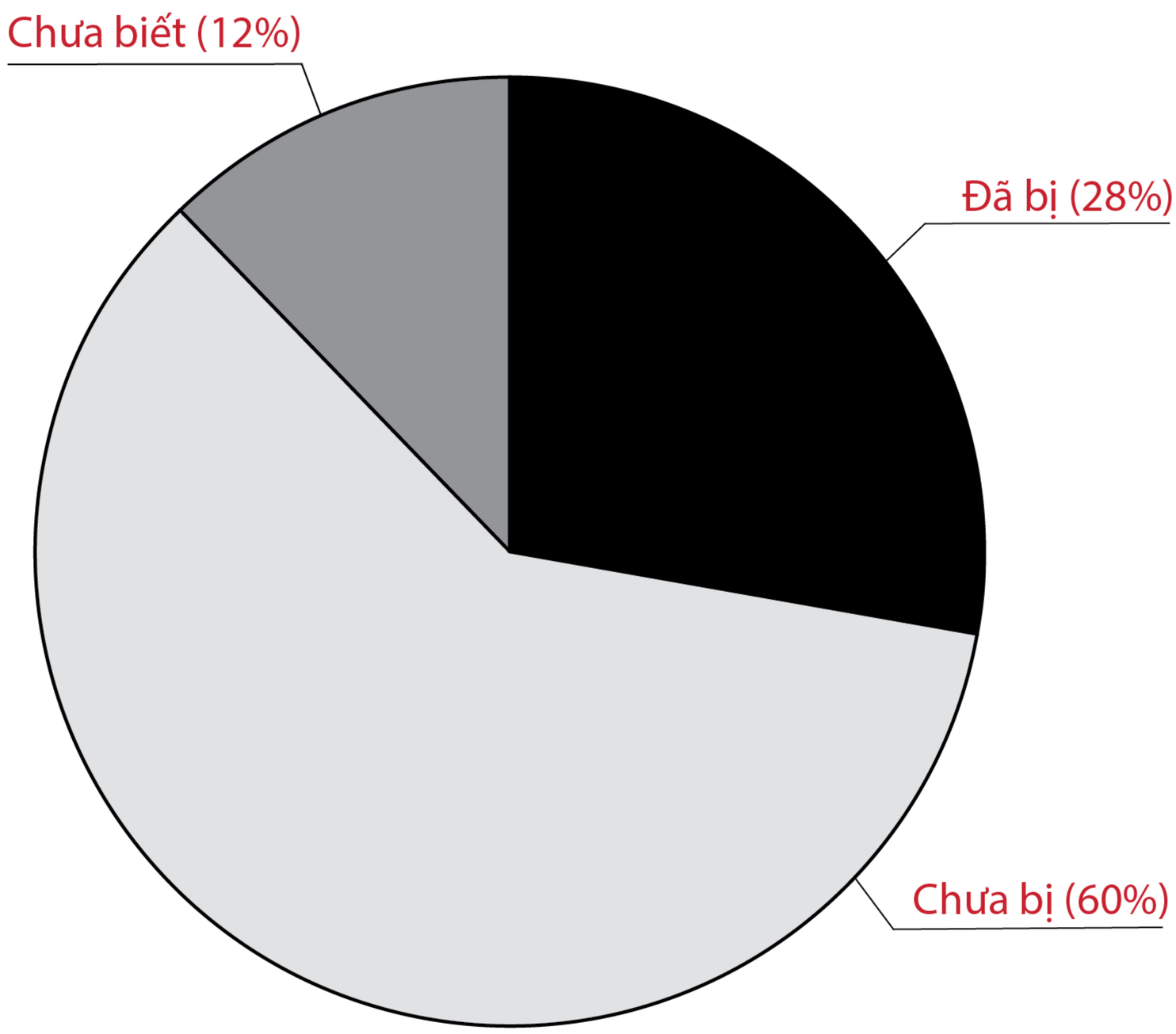
*COVID-19 đã buộc các công ty phải cho nhân viên làm việc từ xa và hoạt động trên các nền tảng cloud. Việc triển khai 5G đã làm cho các thiết bị được kết nối nhanh hơn, tốt hơn, được kết nối nhiều hơn bao giờ hết. Tất cả những điều này nói lên rằng, ngành công nghiệp an ninh mạng đang trở nên quan trọng hơn bao giờ hết. Những sự kiện gần đây và các số liệu thống kê an ninh mạng dưới đây phản ảnh thực trạng an ninh mạng và dự đoán viễn cảnh thời gian tới.*

Covid-19 là tác nhân làm tăng **238%** các vụ tấn công vào ngân hàng

Hacker tấn công mỗi 39 giây, tổng cộng trên **2244** lần trên 1 ngày.

Chi phí bị tổn thất do các cuộc tấn công an ninh mạng sẽ lên tới con số **6.000** tỉ dollar mỹ trong năm 2021

**95%** các lỗi là gây ra do sai sót của con người.

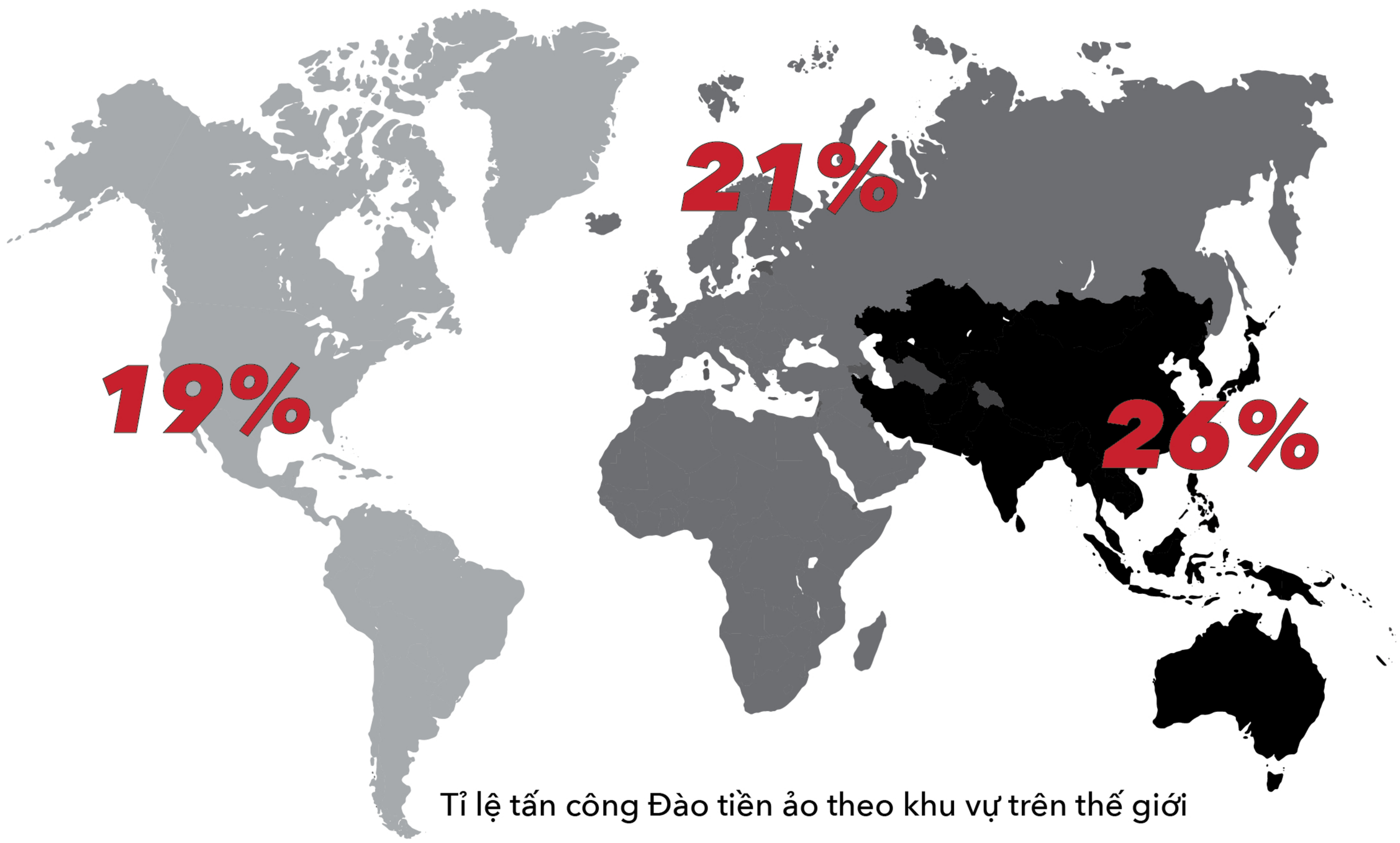



# Khảo sát các tổ chức về hình thức tấn công lợi dụng tình hình dịch Covid-19

Covid 19 không chỉ gây nên sự đình trệ trong kinh tế tài chính, mà còn là cơ hội cho các hacker và tin tặc lợi dụng để tiến hành các cuộc tấn công. Các hacker giả danh các tổ chức y tế hay chính quyền, lừa đảo các nạn nhân để họ bị nhiễm các malware virus độc hại. Việc tính toán thời gian tỉ mỉ cùng lúc với sự bùng phát của virus làm cho các cuộc tấn công này hiệu quả hơn bao giờ hết.

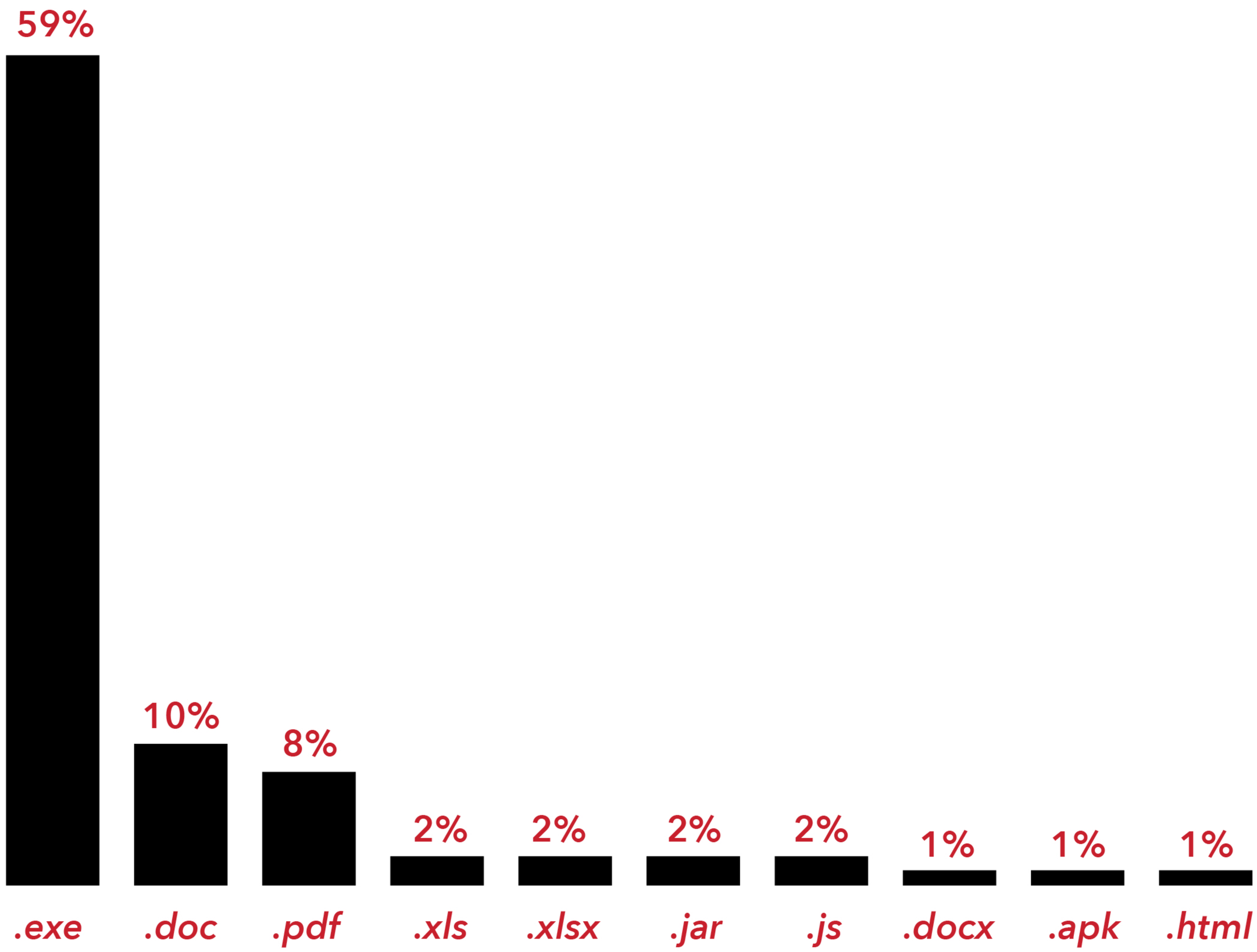

# XU HƯỚNG TẤN CÔNG

Hiện nay, tin tặc không còn đơn thuần tấn công mà âm thầm xâm nhập và khống chế thiết bị của nạn nhân và biến nó thành một zombie - máy sẽ nằm trong sự kiểm soát của chúng. Tập hợp các máy zombie sẽ tạo thành hệ thống botnet, bị điều khiển nhằm vào nhiều mục đích tấn công như: từ chối dịch vụ phân tán (DDoS) và đào tiền ảo. Các tin tặc thường lợi dụng tài nguyên của máy nạn nhân để thực hiện mục đích đào tiền ảo - một trong những xu hướng rất phát triển hiện nay.




Tỉ lệ tấn công Đào tiền ảo theo khu vực trên thế giới

Các nước đang phát triển vẫn là mục tiêu lớn nhất của các cuộc tấn công an ninh mạng do trình độ kỹ thuật chuyên môn cũng như nhân lực còn thiếu thốn, điều này khiến chúng ta phải cảnh giác hơn bao giờ hết.




Biểu đồ thể hiện các dạng file có khả năng bị nhiễm mã độc nhiều nhất.

Các file executable hay .exe vẫn đã và đang là một trong những file có khả năng bị nhiễm malware nhiều nhất. Do bản chất là các file thực thi, đuôi .exe sẽ yêu cầu quyền administrator và sau đó dùng quyền này để tiến hành các cuộc tấn công mà không bị ràng buộc.

# TÌNH HÌNH AN NINH MẠNG TẠI VIỆT NAM

Nhờ các nỗ lực của Nhà nước Việt Nam, nâng cao nhận thức về bảo mật an toàn thông tin và đưa ra các đạo luật phòng chống các cuộc tấn công an ninh mạng, số lượng các cuộc tấn công mạng nhằm vào Việt Nam trong quý I/ 2021 so với năm ngoái đã giảm 14,2% xuống còn 64,35 triệu.

Trung tâm giám sát an toàn không gian mạng quốc gia (NCSC) cho thấy sự tiến bộ trong công tác bảo mật thông tin tại các cơ quan, đơn vị khi triển khai mô hình bốn lớp theo hướng dẫn của Chính phủ.

Chiến dịch do NCSC phối hợp với các doanh nghiệp thuộc Liên minh phòng chống phần mềm độc hại và xử lý tấn công mạng đã đạt được mục tiêu giảm 50% các trường hợp lây nhiễm phần mềm độc hại và giảm một nửa số địa chỉ IP của Việt Nam trong các mạng botnet.

Đây là thành công rực rỡ của sự kiện một phần do các chuyên gia an ninh mạng của Bộ Thông tin và Truyền thông (Bộ TT&TT), Bộ Công an, Bộ Quốc phòng và các doanh nghiệp cung cấp dịch vụ.

# Tài liệu tham khảo:


- https://www.ntsc.org/assets/pdfs/cyber-security-report-2021.pdf
- https://www.cira.ca/cybersecurity-report-2021
- https://www.varonis.com/blog/cybersecurity-statistics/
- https://opengovasia.com/vietnams-major-cybersecurity-initiatives-over-the-last-year/

*VinaAspire®*

Tel: +84 944 004 666 | Fax: +84 28 3535 0668
Email: info@vina-aspire.com

**WWW.VINA-ASPIRE.COM**