NCS
PROTECT YOUR SUCCESS

BÁO CÁO TÌNH HÌNH AN NINH MẠNG VIỆT NAM 2024

- Tổng quan về tình hình an ninh mạng 2024
- Thống kê, phân tích chi tiết và khuyến nghị
- Dự đoán xu hướng 2025

“Báo cáo tình hình an ninh mạng Việt Nam 2024” được Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS) biên soạn với sứ mệnh chia sẻ tri thức, nâng cao nhận thức về an toàn thông tin, và hỗ trợ các tổ chức trong việc đối phó với những thách thức an ninh mạng hiện nay. Thông qua báo cáo, NCS mong muốn đồng hành cùng cộng đồng và các doanh nghiệp trong hành trình xây dựng một môi trường số an toàn, minh bạch và bền vững.

Là đơn vị dẫn đầu trong lĩnh vực an ninh mạng tại Việt Nam, NCS cam kết cung cấp các giải pháp & dịch vụ bảo mật tiên tiến và phù hợp nhất. Báo cáo tổng hợp dữ liệu từ hoạt động thực tế, kết hợp cùng các nguồn thông tin đáng tin cậy, với mục tiêu là hỗ trợ cộng đồng trong việc ứng phó với rủi ro an ninh thông tin ngày càng phức tạp.

CÔNG TY CỔ PHẦN CÔNG NGHỆ AN NINH MẠNG QUỐC GIA VIỆT NAM

(NCS)

PHỤ LỤC

Về NCS

CÔNG TY CỔ PHẦN CÔNG NGHỆ AN NINH MẠNG QUỐC GIA VIỆT NAM (NCS)

Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS) là đơn vị hàng đầu trong lĩnh vực an toàn thông tin, cung cấp các dịch vụ bảo mật toàn diện và tiên tiến. Với mục tiêu bảo vệ tối ưu cho các tổ chức và doanh nghiệp trong quá trình chuyển đổi số, các gói dịch vụ của NCS kết hợp các phương pháp công nghệ hiện đại và chuyên sâu để đáp ứng mọi nhu cầu an ninh mạng. Đội ngũ chuyên gia giàu kinh nghiệm của NCS luôn sẵn sàng đồng hành, đảm bảo hệ thống công nghệ thông tin của khách hàng được bảo vệ an toàn trước mọi thách thức.

Các dịch vụ chuyên sâu về An ninh mạng của NCS được thị trường đánh giá cao, bao gồm: Dịch vụ Kiểm thử xâm nhập hệ thống và ứng dụng (Penetration Testing), Dịch vụ Rà soát và phân tích mã độc (Malware Analysis), Dịch vụ Kiểm thử tấn công xâm nhập chuyên sâu hạ tầng CNTT (Red Teaming), Dịch vụ Điều tra và ứng phó sự cố An ninh mạng (Incident Response), Dịch vụ Tình báo An ninh mạng (Threat Intelligence), và Giải pháp An ninh mạng cho hệ thống Công nghiệp (OT/ICS Security).,….

TẦM NHÌN

NCS luôn nỗ lực trở thành công ty An ninh mạng hàng đầu tại Việt Nam và khu vực, kiến tạo hệ sinh thái bảo mật toàn diện, cung cấp dịch vụ An toàn thông tin chuyên nghiệp, linh hoạt và đạt đẳng cấp quốc tế.

SỨ MỆNH

NCS mang trong mình sứ mệnh xây dựng một không gian mạng an toàn, linh hoạt, đồng hành và bảo vệ cho sự thành công của mọi tổ chức và doanh nghiệp trong hành trình chuyển đổi số.

Tổng quan về tình hình An ninh mạng 2024

BỐI CẢNH CHUNG

LỖ HỔNG BẢO MẬT VÀ NGUY CƠ BỊ KHAI THÁC

Năm 2024, **Mircosoft phát hành bản vá**

1,020 lỗ hổng bảo mật

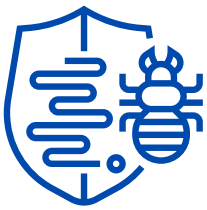
41 lỗ hổng mức độ **Moderate**

951 lỗ hổng mức độ **Important**

28 lỗ hổng mức độ **Critical**

Trên những sản phẩm phổ biến như **Apache, Cisco, Citrix, Vmware, Zabbix, Splunk, Palo Alto, Firefox, Check Point, … Và 12 sản phẩm khác**

SỰ GIA TĂNG MÃ ĐỘC



Ghi nhận được nhiều loại mã độc

- **CobaltStrike**
- **PlugX**
- **Mẫu IIS Backdoor**

Phương thức triển khai mã độc

Chuỗi lây nhiễm phức tạp:

Sử dụng **loader** được viết bằng các ngôn ngữ:

- **Golang**
- **Nim**
- **Rust**
- **Java**

Mẫu mã độc mới:

- Sử dụng **trampoline** để gọi qua lại giữa nhiều DLL.
- Mỗi DLL thực hiện nhiệm vụ/module riêng. Sau đó, các module được gộp thành **file DLL lớn**.

SỰ GIA TĂNG CHIẾN DỊCH TẤN CÔNG CÓ CHỦ ĐÍCH

Mục tiêu tấn công mạng tại Việt Nam

- **Năng lượng**
- **Tài chính**
- **Chính phủ**
- **Hàng không**
- **Dầu khí**

Phương pháp tấn công:

1. Khai thác lỗ hổng bảo mật

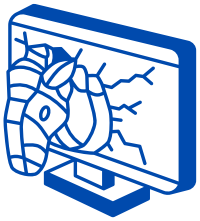
- **Microsoft Exchange.**
- **Oracle Weblogic.**
- **Citrix**

2. Phát tán email lừa đảo (phishing).

3. Tận dụng tài khoản bị rò rỉ.

BỐI CẢNH CHUNG

BIẾN THỂ MOBILE BANKING TROJAN NHẮM VÀO VIỆT NAM



Cuối năm 2023, xuất hiện mã độc **Goldigger** tấn công hơn **50** **ứng dụng tài chính và ví điện tử**

- Mã độc này được phát tán qua các **trang web giả mạo Google Play Store** và các **tệp APK lừa đảo**
- Khai thác **tính năng trợ năng** để:
  - Đánh cắp thông tin đăng nhập ngân hàng.
  - Chặn bắt tin nhắn SMS.
- **Giả mạo ứng dụng hợp pháp** để đánh cắp thông tin tài chính.

Các biến thể mã độc nổi bật:

GoldDiggerPlus	GoldPickaxe	Gigabud	SpyLoan
Nâng cấp với nhiều tính năng mới.	Nhắm mục tiêu cả hệ điều hành Android và iOS.	Giả mạo ứng dụng hợp pháp để đánh cắp dữ liệu tài chính.	• Giả dạng ứng dụng vay tiền trực tuyến để thu thập dữ liệu nhạy cảm. • Gia tăng mạnh mẽ trên phạm vi toàn cầu.

XU HƯỚNG GIA TĂNG HOẠT ĐỘNG CỦA TỘI PHẠM MẠNG

Mục tiêu của các nhóm tấn công mạng:
- Đánh cắp thông tin trình duyệt.
- Tài khoản Facebook
- Thông tin nhạy cảm khác để thu lợi tài chính.

Mã độc nổi bật:
- **Braodo Stealer**
- **VietCredCare**
- **SteelFox**
- **PXA Stealer**

VietCredCare cung cấp dịch vụ dưới hình thức **stealer-as-a-service** , xâm nhập dữ liệu của:

9 **Cơ quan Chính phủ Việt Nam**

12 **Cổng dịch vụ công Quốc gia của tỉnh/thành phố**

65 **Trường Đại học**

21 **Ngân Hàng**

4 **Sàn thương mại điện tử**

Nhiều **Doanh nghiệp lớn**

44/63 **Tỉnh thành**

Thống kê, phân tích chi tiết và khuyến nghị

1. Công nghệ, nền tảng ảnh hưởng nhiều nhất

Trong năm 2024, tại Việt Nam và khu vực chứng kiến sự leo thang chưa từng có của các hoạt động tấn công mạng nhắm vào các nền tảng, thiết bị và phần mềm phổ biến. Các báo cáo toàn cầu đã chỉ ra rằng các hacker không chỉ tận dụng lỗ hổng bảo mật mới mà còn tái sử dụng các công cụ và phương pháp cũ, làm tăng mức độ phức tạp và khó khăn trong việc phòng thủ. Xu hướng này không chỉ đặt ra mối đe dọa đối với các tổ chức toàn cầu mà còn ảnh hưởng sâu rộng đến khu vực châu Á – Thái Bình Dương (APAC) và Việt Nam.

1.1. Lỗ hổng liên quan tới các thiết bị biên - "cửa ngõ" dẫn vào mạng nội bộ

Thiết bị biên, bao gồm VPN, máy chủ email và thiết bị định tuyến văn phòng nhỏ, là một trong những mục tiêu hàng đầu của các nhóm tin tặc, các lỗ hổng trong thiết bị của Fortinet, Palo Alto, Ivanti VPN… đã dẫn đến hàng trăm cuộc xâm nhập, cho phép tin tặc kiểm soát mạng nội bộ. Chỉ riêng năm 2024, chúng tôi thống kê đã có 14 lỗ hổng liên quan đến thiết bị biên bị khai thác, dẫn đến việc xây dựng các mạng botnet khổng lồ như GobRAT và Natwalk. Những mạng botnet này không chỉ được sử dụng để thực hiện các cuộc tấn công từ chối dịch vụ (DDoS) mà còn để triển khai mã độc trên quy mô lớn, gây thiệt hại lớn cho các tổ chức.

Các giao diện quản lý từ xa cho các thiết bị biên như FortiManager, Versa Director, Palo Alto… đã được sử dụng làm cửa ngõ để tin tặc xâm nhập sâu hơn vào mạng nội bộ tổ chức . Phương pháp này đặc biệt nguy hiểm vì nó cho phép kẻ tấn công kiểm soát trực tiếp các hệ thống quan trọng mà không cần xâm nhập qua các lớp bảo mật khác. Điều này cho thấy các tổ chức cần chú trọng vào bảo mật các giao diện quản lý từ xa, đồng thời kiểm tra cấu hình định kỳ để ngăn chặn các lỗ hổng

1.2. Lộ lọt dữ liệu người dùng tại Việt Nam – mối hiểm hoạ khôn lường

Không chỉ ở Việt Nam, mà trên thế giới nói chung đang chứng kiến xu hướng tội phạm mạng **chuyển từ việc hack tài khoản trực tuyến (bẻ khóa, thâm nhập trái phép) sang sử dụng dữ liệu tài khoản có sẵn hoặc được rao bán trên Internet hay Darkweb.**

Năm 2024, tình trạng rao bán và lộ lọt dữ liệu của các cá nhân, tổ chức tại Việt Nam diễn biến phức tạp, với số lượng lên tới hàng trăm triệu bản ghi và hàng chục GB dữ liệu được chia sẻ, rao bán trên các trang chợ đen, diễn đàn ngầm, và Darkweb. Các thông tin bị rao bán thường bao gồm từ dữ liệu cá nhân của người dùng (thông tin tài khoản ngân hàng, hồ sơ eKYC, dữ liệu giao dịch, …) đến các dữ liệu nhạy cảm của công ty, tổ chức (thông tin truy cập hệ thống, tài liệu chiến lược, …).

Sau khi mua hoặc lấy cắp các thông tin tài khoản này, hacker thường sử dụng chúng để thực hiện các hành vi tiếp theo như:

- Gian lận tài chính: Sử dụng thông tin tài khoản ngân hàng để chuyển tiền trái phép hoặc thực hiện các giao dịch bất hợp pháp.
- Tấn công nhắm mục tiêu (Targeted Attacks): Khai thác thông tin để thực hiện các chiến dịch tấn công có chủ đích như phishing, spear phishing hoặc ransomware nhằm vào các cá nhân hoặc tổ chức cụ thể.
- Lạm dụng danh tính (Identity Theft): Sử dụng thông tin cá nhân để tạo tài khoản giả mạo, thực hiện hành vi gian lận hoặc vay tín dụng.
- Bán lại thông tin: Thông tin có giá trị cao có thể tiếp tục được bán lại nhiều lần trên các diễn đàn chợ đen, làm kéo dài chuỗi tội phạm mạng.

Các nguyên nhân chính dẫn đến việc lộ lọt, thất thoát dữ liệu của cá nhân, tổ chức được đội ngũ NCS ghi nhận bao gồm:

- Máy tính cá nhân bị nhiễm mã độc: Chủ yếu là các loại malware đánh cắp thông tin (info-stealer), tập trung vào các thông tin đăng nhập được lưu trên trình duyệt. Nguyên nhân phổ biến là người dùng thiếu cẩn trọng khi cài đặt phần mềm không rõ nguồn gốc hoặc mở các email lạ.
- Lỗ hổng trong hệ thống công ty: Các hệ thống không được quản lý chặt chẽ, tồn tại lỗ hổng bảo mật, là điểm yếu để hacker khai thác nhằm xâm nhập và đánh cắp dữ liệu.

Thực trạng này đặt ra yêu cầu cấp thiết trong việc nâng cao nhận thức bảo mật cho cá nhân và tổ chức, đồng thời triển khai các biện pháp bảo vệ như sử dụng phần mềm bảo mật, kiểm tra và vá lỗ hổng hệ thống định kỳ.

1.3. Các ứng dụng web public – mục tiêu chính của các cuộc tấn công mạng

Trong năm 2024, các ứng dụng web tiếp tục trở thành mục tiêu ưu tiên hàng đầu của các nhóm tin tặc, với hàng loạt lỗ hổng bảo mật bị khai thác để xâm nhập và kiểm soát hệ thống. Một số lỗ hổng phổ biến nhất bao gồm **SQL Injection, Cross-Site Scripting (XSS), và Remote File Inclusion (RFI)**. Các lỗ hổng này thường xuất phát từ việc ứng dụng không được kiểm tra bảo mật kỹ lưỡng hoặc không tuân thủ các nguyên tắc lập trình an toàn.

Đặc biệt, lỗ hổng **SQL Injection** đã được tận dụng để truy xuất thông tin nhạy cảm từ cơ sở dữ liệu, bao gồm thông tin khách hàng, tài khoản người dùng và thậm chí là mã hóa mật khẩu. Một số trường hợp nghiêm trọng ghi nhận việc tin tặc sử dụng lỗ hổng này để tạo tài khoản quản trị trái phép hoặc chiếm quyền kiểm soát toàn bộ hệ thống. Lỗ hổng XSS cũng được khai thác để thực hiện các cuộc tấn công lừa đảo hoặc phát tán mã độc tới người dùng hợp pháp thông qua các kịch bản được nhúng trực tiếp vào ứng dụng web.

Ngoài ra, một trong những lỗ hổng đáng chú ý là từ tính năng **Upload File** trên các ứng dụng web. Tin tặc sử dụng các phương pháp vượt qua kiểm tra file để tải lên các tệp độc hại, chẳng hạn như webshell, cho phép chúng thực hiện lệnh trực tiếp trên máy chủ. Điều này gây rủi ro nghiêm trọng, không chỉ làm rò rỉ dữ liệu mà còn khiến hệ thống dễ dàng bị kiểm soát toàn diện.

Việc thiếu cập nhật phần mềm và vá lỗi kịp thời cũng là một yếu tố quan trọng khiến nhiều tổ chức trở thành nạn nhân. Các nền tảng ứng dụng web như **PHP, WordPress, và ASP.NET** thường bị khai thác do sử dụng các phiên bản cũ không còn được hỗ trợ. Bên cạnh đó, cấu hình sai hoặc không tuân thủ các tiêu chuẩn an toàn, chẳng hạn việc mở rộng quyền truy cập hoặc không sử dụng mã hóa HTTPS, càng làm tăng nguy cơ.

Năm qua đã cho thấy các lỗ hổng bảo mật trong ứng dụng web không chỉ là thách thức kỹ thuật mà còn là bài toán chiến lược trong quản lý an ninh mạng. Việc nâng cao nhận thức bảo mật, áp dụng các công cụ kiểm tra lỗ hổng tự động, và thực hiện vá lỗi định kỳ là những bước cần thiết để bảo vệ các ứng dụng web khỏi sự khai thác của tin tặc.

1.4. Mối đe doạ từ các cuộc tấn công nhắm vào máy chủ Microsoft Exchange

Với mức độ phổ biến của Microsoft Exchange tại Việt Nam trong các tổ chức từ chính phủ đến doanh nghiệp khiến các máy chủ Microsoft Exchange tiếp tục là một trong những mục tiêu tấn công chính của nhiều nhóm tin tặc. Lỗ hổng nổi bật như ProxyLogon và ProxyNotShell đã bị khai thác để drop webshell, cung cấp quyền truy cập ban đầu vào hệ thống Exchange. Một khi truy cập thành công, tin tặc thay đổi mã nguồn ứng dụng để thu thập thông tin người dùng trong quá trình đăng nhập. Với thông tin đăng nhập này, chúng tiếp tục triển khai các công cụ như WmiPrvSe.exe để mở rộng tấn công sang các hệ thống liên quan.

Ngoài ra, các cuộc tấn công thường thay đổi cấu hình web.config trên máy chủ Exchange, hướng tới các tệp thực thi mã độc được lưu trữ trước đó. Mã độc này cho phép đọc request và response trên máy chủ, từ đó trích xuất tài khoản email và mã hóa dữ liệu bằng định dạng Base64, lưu trữ dưới dạng các tệp tin định dạng .dat. Hoạt động này không chỉ tạo điều kiện cho các chiến dịch gián điệp mà còn có thể làm rò rỉ thông tin nhạy cảm như email của lãnh đạo, kế hoạch kinh doanh, và các tài liệu pháp lý quan trọng.

Khi khai thác thành công, tin tặc không chỉ đánh cắp dữ liệu mà còn có thể sử dụng máy chủ email bị xâm phạm làm bàn đạp để phát tán mã độc qua các email phishing hoặc điều phối các cuộc tấn công phức tạp hơn trong toàn mạng lưới.

2. APT, Campaign, Malware

2.1. Các chiến dịch tấn công APT diễn ra mạnh mẽ trong năm 2024

2.1.1. Các cuộc tấn công nổi bật nhắm mục tiêu các đơn vị, tổ chức của Việt Nam

Trong quá trình điều tra, xử lý sự cố an ninh mạng cho các tổ chức, đơn vị tại Việt Nam trong năm vừa qua, chúng tôi tổng hợp lại một số kịch bản tấn công phổ biến theo các lĩnh vực như sau

NHÀ NƯỚC

Kẻ tấn công triển khai mã độc CobaltStrike và các công cụ tấn công trên máy chủ máy trạm của nhiều hệ thống. Sử dụng kỹ thuật Domain Fronting nhằm che giấu kết nối tới C2

Máy chủ sử dụng Telerik phiên bản thấp cho phép kẻ tấn công upload webshell, thu thập thông tin hệ thống

Kẻ tấn công khai thác lỗ hổng trong Oracle Weblogic, drop webshell cùng các công cụ tấn công khác

TÀI CHÍNH

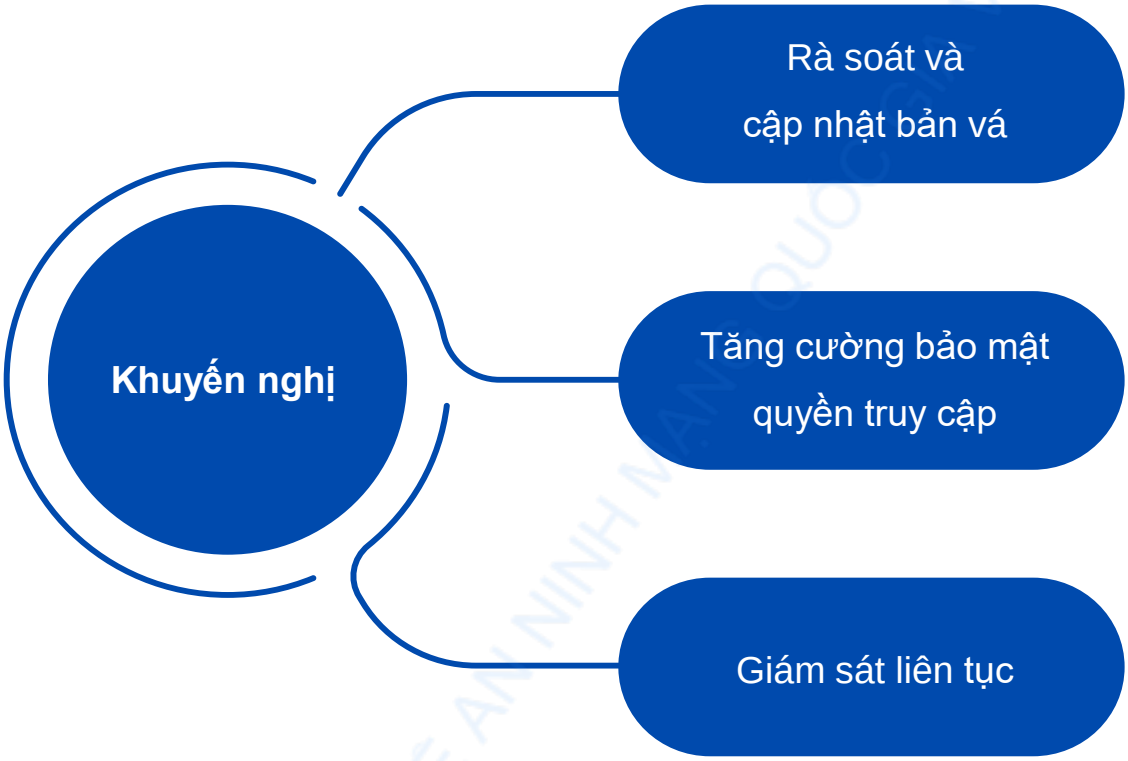
Kẻ tấn công khai thác các lỗ hổng bảo mật trên các ứng dụng web, triển khai keylogger trên các máy máy trạm nắm giữ tài khoản quan trọng, sử dụng để tấn công các hệ thống khác

Khai thác cấu hình yếu trong ViewState, từ đó drop webshell, trích xuất thông tin xác thực lsass và triển khai mã độc trên hệ thống

NĂNG LƯỢNG

Tấn công hệ thống máy chủ Exchange
• Thông qua khai thác lỗ hổng bảo mật ProxyLogon, kẻ tấn công drop webshell để có quyền truy cập ban đầu. Để thu thập thông tin tài khoản, kẻ tấn công thay đổi source code ứng dụng nhằm thu thập thông tin người dùng khi đăng nhập. Với các thông tin xác thực thu được, kẻ tấn công sử dụng để WmiPrvSe.exe tấn công sang hệ thống khác. • Kẻ tấn công drop mã độc xuống đường dẫn \bin trên hệ thống Exchange, thay đổi cấu hình web.config trỏ tới tệp tin mã độc thực thi mã độc. Mã độc thực hiện đọc request, response của trên máy chủ Exchange để truy xuất tài khoản email Exchange, mã hóa base64 và ghi thông tin vào các tệp tin định dạng .dat
Các sự cố bắt nguồn từ lộ lọt tài khoản VPN
• Kẻ tấn công thực hiện truy cập vào hệ thống, dò quét, chiếm quyền các hệ thống khác trong mạng, thu thập thông tin và sử dụng DCSync tấn công máy chủ DC • Kẻ tấn công triển khai mã độc CobaltStrike, trích xuất thông tin xác thực lsass, tắt service logs Sysmon, xóa logs nhằm tránh bị phát hiện • Thông qua chiếm quyền điều khiển máy trạm, kẻ tấn công tấn công máy chủ sử dụng WMI, dò quét và trích xuất thông tin xác thực từ tiến trình lsass.exe sử dụng procdump
Các sự cố liên quan đến khai thác các lỗ hổng bảo mật ứng dụng web
• Khai thác lỗ hổng SQL Injection, thông qua thành phần có sẵn của Microsoft certutil.exe để tải xuống các tệp tin độc, revershell thông qua powershell • Khai thác lỗ hổng thông qua cấu hình yếu trên phiên bản ASP.NET đang sử dụng có thể thực thi lệnh, upload file tùy ý. Từ đó tạo các tài khoản và thêm vào nhóm đặc quyền administrator, tải lên các công cụ hỗ trợ như reverse proxy, remote tool. • Máy chủ chạy ứng dụng web tồn tại lỗ hổng trong tính năng UpLoadFile, cho phép kẻ tấn công upload file tùy ý, kẻ tấn công sau khi có được webshell thực hiện thu thập thông tin hệ thống
Kẻ tấn công triển khai mã độc dưới dạng dịch vụ, load các DLL, giải mã cấu hình C2 bằng thuật toán chacha20 Thu thập thông tin hệ thống, tài khoản domain, thay đổi mật khẩu tài khoản và xóa logs để gây khó khăn trong quá trình truy vết
Người dùng nhận được email phishing sử dụng kỹ thuật GrimResource giả mạo công văn nhằm mã độc trên máy nạn nhân, thu thập thông tin và triển khai thêm mã độc CobaltStrike

KHUYẾN NGHỊ



1. Rà soát và cập nhật bản vá: Chủ động kiểm tra và vá lỗi các hệ thống sử dụng các ứng dụng và thiết bị phổ biến bị khai thác, như Microsoft Exchange, Citrix, và Oracle.

2. Tăng cường bảo mật quyền truy cập: Áp dụng xác thực đa yếu tố (MFA) và thực thi nguyên tắc quyền truy cập tối thiểu (Least Privilege) để giảm thiểu rủi ro khi tài khoản bị xâm phạm.

3. Giám sát liên tục: Triển khai các hệ thống giám sát và phát hiện mối đe dọa (SIEM, EDR) để kịp thời nhận diện và phản ứng với các hành vi bất thường trong mạng.

2.1.2. Các hoạt động tấn công mạng vào các tổ chức tại Việt Nam từ các nhóm tấn công được cho liên kết với nhóm tấn công nước ngoài

Trong năm 2024, đội ngũ Threat Intelligence (TI) của NCS đã ghi nhận và xử lý nhiều sự cố an ninh mạng, đồng thời phân tích thông tin từ các cuộc tấn công nhắm vào các tổ chức thuộc nhiều lĩnh vực trên lãnh thổ Việt Nam.

a. Các kỹ thuật tấn công phổ biến

Dựa trên quá trình thu thập và phân tích dữ liệu, đội ngũ chuyên gia của NCS đã tổng hợp các kỹ thuật tấn công phổ biến nhất được sử dụng trong năm qua. Những phát hiện từ các công cụ, kỹ thuật, và cơ sở hạ tầng liên quan cho thấy dấu hiệu của nhiều cuộc tấn công có khả năng được thực hiện bởi các nhóm APT, trong đó nổi bật là những nhóm được cho là có nguồn gốc từ Trung Quốc.

Khởi tạo truy cập

Để khởi tạo truy cập ban đầu, các nhóm tấn công sử dụng chủ yếu các phương pháp chính sau:

- **Khai thác các lỗ hổng bảo mật trên các ứng dụng, thiết bị phổ biến** như Microsoft Exchange (Proxy Logon, ProxyNotShell), Oracle (CVE-2017-10271, CVE-2022-21587), Citrix NetScaler ADC, Citrix Gateway, Zimbra Collaboration Suite, Ciso ASA SSL VPN, Veeam Backup, hầu hết đều facing ra môi trường Internet. Ngoài ra có các lỗ hổng khác tồn tại trên các thành phần như Telerik (CVE-2017-22317, CVE-2017-11357, CVE-2019-18935, CVE-2019-18935), ViewState hoặc mã nguồn tự phát triển có các lỗ hổng cho phép vượt qua xác thực (bypass authentication), upload file tùy ý.
- **Gửi email lừa đảo (phishing): g**ửi các email lừa đảo, nội dung trong hòm thư thường đính kèm tệp tin nén độc hại hoặc đường dẫn trỏ đến nơi lưu trữ các tệp tin độc hại.
- **Sử dụng thông tin tài khoản bị lộ:** Nhóm tấn công thu thập thông tin tài khoản, mật khẩu từ các nguồn như **dark web**, **stealer malware**, hoặc dữ liệu rò rỉ. Sau đó, chúng sử dụng thông tin này để truy cập trái phép vào các hệ thống.

Post Exploitation: Một số hình thái của các nhóm tấn công sau khi có quyền truy cập ban đầu nhằm duy trì chỗ đứng trong hệ thống (persistence), thu thập thông tin xác thực và tấn công ngang hàng sang các hệ thống khác trong mạng.

Mã độc – Malware: Năm 2024, NCS TI ghi nhận nhiều loại mã độc được sử dụng trong quá trình tấn công, phổ biến nhất là CobaltStrike, Plugx và các mẫu IIS Backdoor. Các nhóm tấn công áp dụng các chuỗi lây nhiễm khác nhau trong giai đoạn đầu để drop các loader sử dụng đa dạng các ngôn ngữ lập trình như Golang, Nim, Rust và Java nhằm triển khai các mã độc, nổi bật:

CobaltStrike: Với việc cung cấp nền tảng cho phép dễ quản lý và thao tác, mã độc được sử dụng phổ biến trong các cuộc tấn công. Trong các cuộc tấn công, hầu hết mã độc CobaltStrike sẽ được gọi và giải mã bởi nhiều tệp tin độc hại khác ở nhiều giai đoạn trước khi được triển khai trong bộ nhớ của máy nạn nhân, cụ thể như:

- Sử dụng cách thức tấn công mới có tên GrimResource thực thi VBScript độc hại thông qua mmc.exe, từ đó tải xuống và thực thi trong bộ nhớ các tệp tin độc hại khác được lưu trữ trên máy chủ C&C của kẻ tấn công. Sau khi tạo kết nối tới máy chủ C&C, mã độc thu thập thông tin hệ thống trên máy nạn nhân và triển khai thêm mã độc CobaltStrike. Chiến dịch tấn công nhắm đến 1 đơn vị thuộc ngành năng lượng tại Việt Nam, qua phân tích đội ngũ TI NCS đánh giá nhóm tấn công đứng đằng sau có nguồn gốc từ Trung Quốc.
- Thông qua DLL SideLoading, lạm dụng các tệp tin thực thi hợp pháp để gọi tới các DLL độc hại cùng đường dẫn, DLL độc hại thực hiện giải mã tệp tin thu được payload là CobaltStrike, một số mẫu mã độc khác với loader được viết bằng ngôn ngữ Go thực hiện nhiều giai đoạn giải mã (DES(AES(RC4))) trước khi triển khai mã độc CobaltStrike trong bộ nhớ.
- Một hình thái khác để triển khai mã độc CobaltStrike là sử dụng tệp tin định dạng .jar và được thực thi thông qua tiến trình java.exe. Bên trong .jar chứa class có nhiệm vụ giải mã, nhả (drop) và thực thi CobaltStrike.

PlugX và các biến thể:

- Ngoài phương thức đã được biết sử dụng các tệp tin định dạng .lnk trong giai đoạn đầu, đội ngũ NCS cũng đã phát hiện kỹ thuật GrimResource được sử dụng để tải xuống và thực thi các tệp tin định dạng .msi. Loader được viết bằng ngôn ngữ Nim có nhiệm vụ giải mã và triển khai mã độc PlugX, các chiến dịch ghi nhận nhắm tới lực lượng vũ trang, đơn vị nhà nước, Chính phủ thuộc Việt Nam dựa theo tài liệu decoy. Phân tích hành vi và cơ sở hạ tầng cũng cho thấy các dấu hiệu nhóm thực hiện tấn công có nguồn gốc từ Trung Quốc (có thể có liên quan đến Mustang Panda).
- Một số biến thể khác của PlugX như THOR, DOPLUGS có thêm một số module hỗ trợ thêm cho qua trình tải xuống, được ghi nhận nhắm tới một số người dùng lĩnh vực tài chính, một số mẫu khác ghi nhận được upload trên virustotal từ khu vực Việt Nam.
- Ghi nhận backdoor CBROVER, được sử dụng để triển khai thêm Plugx trên các máy nạn nhân thuộc lĩnh vực tài chính. Mẫu mã độc cũng được ghi nhận trong các bài viết đã xuất bản trên không gian mạng liên quan đến nhóm tấn công Earth Preta.

IIS Backdoor: Cho phép kẻ tấn công tạo kênh kết nối thực thi command, inject custom shellcode, thu thập thông tin đăng nhập, một số mẫu mã độc khác ghi nhận sử dụng cho mục đích SEO, tăng xếp hạng cho các trang web có nội dung cờ bạc.

Ngoài ra, chúng tôi cũng ghi nhận một mẫu mã độc có cách thức viết mới, sử dụng trampoline để gọi qua lại giữa nhiều DLL, mỗi DLL có những nhiệm vụ, module riêng. Sau một khoảng thời gian theo dõi, ghi nhận các module này được gộp chung thành một file DLL với dung lượng file khá lớn.

Các công cụ hỗ trợ tấn công khác: Bên cạnh các backdoor, đội ngũ NCS cũng ghi nhận có trường hợp nhóm tấn công sử dụng các loader để giải mã và triển khai các công cụ hỗ trợ trong quá trình tấn công như reverse proxy frp, scan dải mạng, hầu hết đều là công cụ opensource.

Cơ sở hạ tầng:

- Trong 1 số chiến dịch ghi nhận nhóm tấn công sử dụng kỹ thuật **Domain Fronting** nhằm che dấu địa chỉ C2, các cấu hình này được ghi nhận trong beacon của mã độc CobaltStrike.
- Sử dụng thêm **cơ sở hạ tầng**, domain là môi trường cloud để lưu trữ tệp tin độc hại hoặc C&C server.
- Sử dụng thêm dịch vụ **Cloudflare content delivery network (CDN)** làm proxy chuyển tiếp traffic đến VPS mà kẻ tấn công nắm giữ. Ngoài ra, các tên miền hợp pháp trước đây được nhóm tấn công đăng ký lại thông qua Namecheap sau khi hết hạn với mục đích có thể giúp tăng độ tin cậy.
- Thông qua việc theo dõi dựa theo **TLS certificate** được sử dụng cho C&C của mã độc, phát hiện thêm cơ sở hạ tầng liên quan đến mã độc KEYPLUG, mã độc Pantegana, trong số đó có một số IP ghi nhận có các kết nối tới một số đơn vị tại Việt Nam.

b. i-SOON –Công ty công nghệ được cho là có liên hệ với nhiều nhóm tấn công mạng tại Trung Quốc

Vào đầu năm 2024, NCS TI phát hiện một tài khoản ẩn danh trên Github đã công khai tài liệu và các đoạn hội thoại liên quan đến Anxun (hay còn gọi là i-SOON – 安洵信息技术有限公司), một công ty công nghệ có trụ sở tại Trung Quốc chuyên cung cấp dịch vụ xâm nhập và đào tạo về bảo mật an toàn thông tin cho các tổ chức và đơn vị trong nước.

Qua phân tích các tài liệu bị rò rỉ, i-SOON được cho là đã nhắm mục tiêu vào ít nhất 22 quốc gia, tập trung chủ yếu vào các cơ quan chính phủ, tổ chức viễn thông và giáo dục. Tại Việt Nam, các tổ chức thuộc Chính phủ, doanh nghiệp nhà nước và các lĩnh vực trọng yếu như hàng không, dầu khí có thể đã trở thành mục tiêu hoặc nạn nhân của i-SOON.

Đáng lưu ý, i-SOON không chỉ tập trung vào các hoạt động quốc tế mà còn ưu tiên hỗ trợ các chiến dịch trong nước, nhắm vào các nhóm dân tộc thiểu số, các cộng đồng tôn giáo và cả lĩnh vực "công nghiệp" cờ bạc.

2.2. Tấn công Ransomware gây thiệt hại nghiêm trọng cho nhiều tổ chức, doanh nghiệp Việt Nam

Năm 2024 ghi nhận các cuộc tấn công Ransomware nhắm đến các tổ chức, doanh nghiệp Việt Nam thuộc nhiều lĩnh vực bao gồm tài chính, năng lượng, viễn thông, dịch vụ công và y tế. Các cuộc tấn công này đã gây ra hậu quả nghiêm trọng cho các đơn vị bị nhắm đến, với ước tính thiệt hại lên tới hơn 10 triệu USD.

Đáng chú ý, nhóm **LockBit** thực hiện một cuộc tấn công lớn vào **một công ty tài chính**, làm tê liệt hoàn toàn hệ thống hoạt động, và một cuộc tấn công khác nhắm vào hệ thống thanh toán của một công ty năng lượng, khiến dịch vụ bị đình trệ trong nhiều ngày. Nhóm **Phobos Ransomware** cũng gây thiệt hại đáng kể cho **một công ty bưu chính**, sử dụng công cụ SSHFS để mã hóa dữ liệu trên các ổ lưu trữ chia sẻ. Tin tặc còn khai thác RDP từ các IP bên ngoài để truy cập máy chủ backup, cùng các công cụ như **Mimikatz** và **veeam-creds** để thu thập thông tin xác thực, tạo điều kiện cho các cuộc tấn công leo thang đặc quyền.

Bên cạnh đó, các nhóm **như BlackByte, Kill Security Ransomware, và Knight Ransomware** cũng đã nhắm mục tiêu vào nhiều tổ chức khác nhau tại Việt Nam, làm gia tăng mức độ nghiêm trọng của vấn đề

Khuyến nghị

Những cuộc tấn công này không chỉ gây tổn thất tài chính mà còn là lời cảnh báo mạnh mẽ cho các tổ chức Việt Nam về việc cần xây dựng hệ thống bảo mật mạnh mẽ hơn. Điều này bao gồm kiểm tra thường xuyên các dịch vụ backup, hạn chế quyền truy cập từ xa, và triển khai giám sát liên tục nhằm phát hiện sớm các hành vi đáng ngờ.

2.3. Chiến dịch tấn công nhắm đến các đơn vị, tổ chức Việt Nam sử dụng kĩ thuật GrimResource

Từ cuối tháng 7 đến đầu tháng 9 năm 2024, đội ngũ Threat Intelligence của NCS đã thu thập và phân tích các mẫu mã độc áp dụng kỹ thuật tấn công *GrimResource*. Những cuộc tấn công này nhắm mục tiêu đến nhiều tổ chức và đơn vị tại Việt Nam.

- **Mẫu mã độc đầu tiên** được phát hiện nhắm vào một đơn vị thuộc ngành năng lượng tại Việt Nam. **Phân tích bổ sung** và thông tin từ các nguồn Threat Intelligence khác xác nhận rằng đây là một phần của chiến dịch quy mô lớn. Chiến dịch này nhằm vào các tổ chức thuộc ngành năng lượng, quân sự, và chính phủ tại các quốc gia Đông và Đông Nam Á, bao gồm Việt Nam, Đài Loan, và Hàn Quốc.
- **Mẫu mã độc thứ hai** sử dụng file .msc nhằm triển khai mã độc PlugX nhắm tới các đơn vị Chính phủ tại Việt Nam.

Sample 1

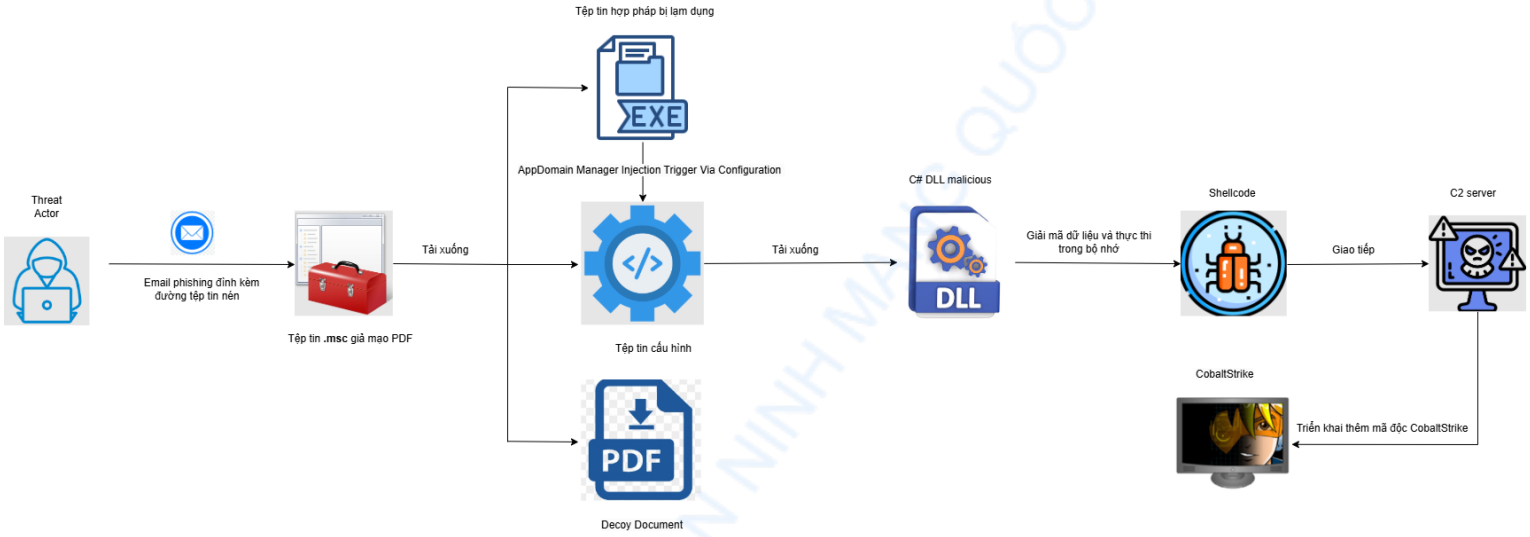
Threat actor khởi tạo tấn công thông qua việc gửi email phishing tới người dùng đính kèm tệp tin được nén trong file .zip.

Kiểm tra email được gửi đến ghi nhận các thông tin:

- Tên email: **Về chỉ đạo và yêu cầu kiểm tra giám sát tình hình hoạt động của các đơn vị thuộc [REDACTED] trong năm 2024**
- Người gửi: **Nguyen Thanh Van <thanhnvs@outlook.com>**
- Tệp tin đính kèm: **Hướng dẫn và yêu cầu kiểm tra, giám sát hoạt động của từng đơn vị năm 2024.zip**

Giải nén tệp tin đính kèm thu được tệp tin định dạng .msc với biểu tượng giả mạo file PDF.

Giải nén tệp tin đính kèm thu được tệp tin định dạng .msc với biểu tượng giả mạo file PDF. Khi người dùng thực hiện mở tệp tin định dạng .msc, các đoạn mã độc hại sẽ được khởi chạy thông qua kĩ thuật tấn công GrimResource, tệp tin decoy v.pdf cũng sẽ được tải xuống từ máy chủ C&C và được mở nhằm lừa nạn nhân, đồng thời thực thi shellcode độc hại trong bộ nhớ của người dùng bị ảnh hưởng.



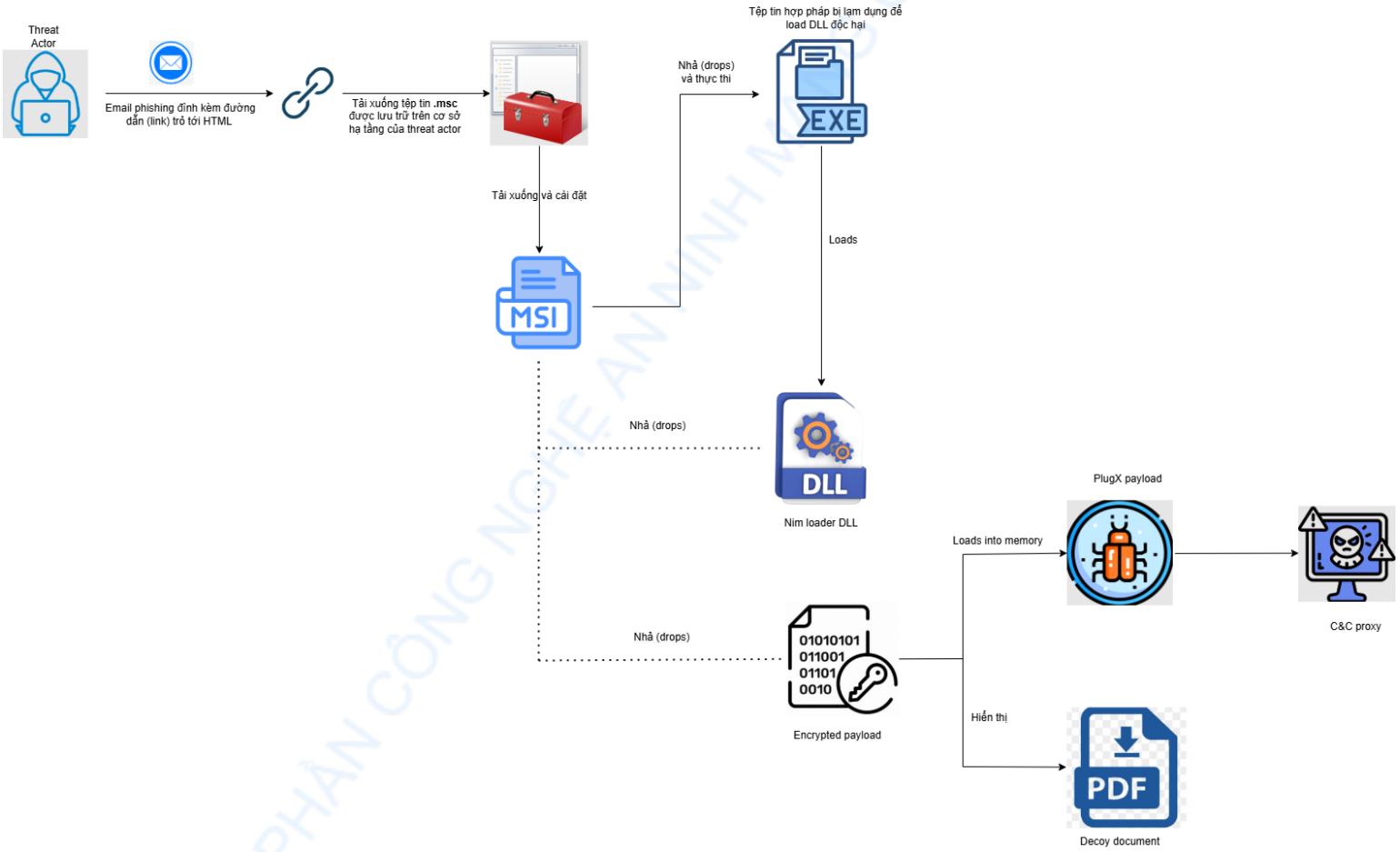
Kĩ thuật tấn công GrimResource thu được trong file .msc gồm các bước:

- Sử dụng biểu tượng giả mạo file .pdf để hiển thị thay cho biểu tượng gốc của file .msc.
- Khai thác lỗ hổng trong aspd.dll để load Javascript URI.
- Sử dụng MSXML method (XSL transformation) và DotNetToScript để thực thi VBScript payload.

Các tệp tin độc hại được tải xuống từ địa chỉ C&C *footracker-statics.s3[.]sa-east-1[.]amazonaws[.]com*, được lưu tại các đường dẫn *C:\User\Public\Music* và *C:\User\Public*. Quá trình thực thi các tệp tin này cũng như các payload kế tiếp dẫn đến mục tiêu cuối cùng là triển khai 1 mẫu mã độc CobalStrike trên máy các nạn nhân (Phân tích chi tiết xem tại *https://ncsgroup.vn/grimresource-in-the-wild-ma-doc-nham-muc-tieu-viet-nam/*).

Sample 2

Đến đầu tháng 09/2024, đội ngũ Threat Intelligence NCS ghi nhận thêm các tệp tin .msc độc hại giả mạo tài liệu sử dụng định dạng PDF và Words có tên file là **Pg 151 vv nghi le Quoc khanh 2.9.msc.1** và **BCTT 02.9 AM Final.docx.msc**. Tuy cùng sử dụng kĩ thuật GrimResource nhưng cách thức triển khai mã độc trong VBScript payload khác với các mẫu trước đó khi threat actor sử dụng WindowsInstaller.Installer, tải xuống mã độc ở phase tiếp theo thông qua method InstallProduct và đặt giá trị UILevel là 2 (Silent Installation).



2.4. Các biến thể Mobile banking Trojan nhắm vào các tổ chức tài chính, ngân hàng Việt Nam

Cuối năm 2023, các báo cáo mô tả về phần mềm độc hại có tên GoldDigger nhắm đến hơn 50 ứng dụng, ví điện tử/tiền điện tử thuộc các tổ chức tài chính tại Việt Nam. Mẫu mã độc được phát tán thông qua các trang web giả mạo nền tảng Google Play Store, các apk mạo danh các đơn vị uy tín tại Việt Nam, lạm dụng tính năng trợ năng trong thiết bị mobile để trích xuất thông tin cá nhân, đánh cắp thông tin đăng nhập ứng dụng ngân hàng, chặn bắt các tin nhắn SMS và thực hiện nhiều hành động khác nhau. Các mẫu mã độc này sử dụng Virbox Protector, một phần mềm hợp pháp cung cấp khả năng che giấu và mã hóa mã nguồn, gây khó khăn trong quá trình phân tích.

Quá trình theo dõi tiếp tục phát hiện mã độc GoldDiggerPlus, GoldKefu và GoldPickaxe được phát triển từ GoldDigger. Trong đó mở rộng các tính năng trong GoldDiggerPlus và GoldKefu cho phép thực hiện các cuộc gọi thoại tới nạn nhân. Với GoldPickaxe, mã độc nhắm đến cả người dùng nền tảng iOS, lạm dụng nền tảng TestFlight của Apple để phát tán mã độc. Một cách thức tấn công khác tinh vi hơn là lừa người dùng sử dụng MDM (Vmware WorkSpace ONE - Mobile Device Management) để kiểm soát các thiết bị của nạn nhân. Mã độc thu thập thông tin cá nhân của người dùng, tin nhắn SMS và dữ liệu nhận dạng khuôn mặt. Để khai thác dữ liệu sinh trắc học bị đánh cắp từ người, kẻ tấn công tạo deepfake thông qua các dịch vụ sử dụng AI hoán đổi khuôn mặt nhằm truy cập trái phép vào tài khoản ngân hàng của nạn nhân.

Quá trình phân tích thêm một số mẫu nhắm tới tổ chức tài chính Bắc Mỹ, trong mã nguồn sau khi decomplier cũng chứa một số thông tin liên quan đến một số tài chính/ngân hàng tại Việt Nam.

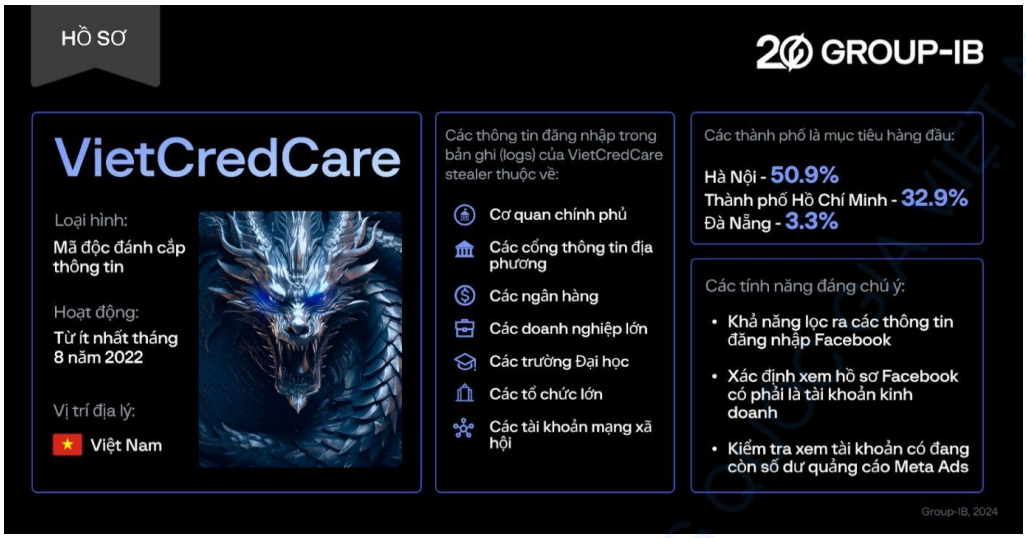
Một loại mã độc khác có tên Gigabud cũng được ghi nhận, giả mạo dưới các ứng dụng hoặc bản cập nhật hợp pháp được thiết kế để chặn bắt thông tin ứng dụng ngân hàng và các dữ liệu nhạy cảm khác, các phân tích cho thấy có những đặc điểm tương đồng với GoldDigger trong mã nguồn .

Ngoài ra, đội ngũ NCS cũng ghi nhận sự gia tăng đáng kể của ứng dụng độc hại SpyLoan trên toàn cầu với hơn 8 triệu lượt cài đặt được phát hiện trên Google Play, cụ thể từ cuối quý 2 đến cuối quý 3 năm 2024, số lượng ứng dụng và thiết bị nhiễm mã độc tăng hơn 75%. Đây là một loại ứng dụng di động giả dạng dưới hình thức các ứng dụng cho vay trực tuyến hoặc dịch vụ tài chính, sau đó bằng các kỹ nghệ xã hội lừa người dùng cung cấp quyền truy cập tin nhắn SMS, lịch sử cuộc gọi, danh bạ và camera. Khi người dùng cấp phép, ứng dụng sẽ thu thập các dữ liệu nhạy cảm như thông tin nhận dạng cá nhân, dữ liệu tài khoản ngân hàng, dữ liệu thiết bị

2.5. Gia tăng hoạt động của các nhóm tội phạm mạng có nguồn gốc từ Việt Nam

Trong năm 2024, gia tăng số lượng các hoạt động tấn công được cho xuất phát từ các nhóm tấn công Việt Nam, phát triển và sử dụng các stealer nhắm mục tiêu chính đến việc ăn cắp thông tin trình duyệt, tài khoản Facebook nhằm thu lợi tài chính từ các hoạt động này. Đặc điểm chung của các threat actor này là sử dụng các ngôn ngữ như Python, C#, thuận lợi cho quá trình phát triển stealer, phát tán mã độc thông qua các tin nhắn hoặc bài đăng lừa đảo trên Facebook và sử dụng các bot của Telegram hoặc Discord làm nơi lưu dữ liệu bị đánh cắp, nổi bật như sau:

- Braodo Stealer, phần mềm đánh cắp thông tin được viết bằng ngôn ngữ Python, nhắm mục tiêu chính là người dùng ở Việt Nam và mở rộng sang các nạn nhân ở Hoa Kỳ, Châu Âu và một số quốc gia châu Á. Được phát tán chủ yếu thông qua các chiến dịch lừa đảo (phishing), Braodo sử dụng các kho lưu trữ mã nguồn mở GitHub và VPS tại Singapore nhằm lưu trữ các tệp tin độc hại. Phần mềm độc hại cho phép đánh cắp dữ liệu từ các trình duyệt khác nhau, bao gồm Chrome, Firefox, Edge và Cốc Cốc thu thập các thông tin đăng nhập đã lưu, cookie và các thông tin khác được lưu trữ trên trình duyệt, một số phiên bản nhắm mục tiêu vào dữ liệu Facebook, thông tin thẻ tín dụng và ví tiền điện tử như Coinbase và Binance.



- VietCredCare, stealer cung cấp theo hình thức stealer-as-a-service, xâm phạm thông tin đăng nhập của người dùng tại 9 cơ quan chính phủ Việt Nam, Cổng dịch vụ công Quốc gia của 12 tỉnh/thành phố, 65 trường Đại học, 4 sàn thương mại điện tử, 21 ngân hàng, 12 doanh nghiệp lớn của Việt Nam cùng với 1 số lượng lớn tài khoản truyền thông, các tổ chức nạn nhân được xác định ở 44 trong số 63 tỉnh thành của Việt Nam. Mục tiêu chính nhắm đến thông tin tài khoản Facebook, đặc biệt là các tài khoản doanh nghiệp, tài khoản có lượng theo dõi cao. Các tài khoản bị đánh cắp có thể bị lợi dụng để đăng tải các nội dung liên quan đến chính trị hoặc thu lợi tài chính thông qua gửi các liên kết lừa đảo, hoặc giao bán thông tin xác thực.
- SteelFox, phần mềm đánh cắp thông tin và khai thác tiền điện tử, giả mạo các phần mềm crack cho các chương trình AutoCAD, JetBrains và Foxit PDF Editor để lây nhiễm SteelFox
- PXA Stealer, phát tán thông qua email lừa đảo, được thiết kế để lấy cắp thông tin nhạy cảm của nạn nhân, bao gồm thông tin đăng nhập của các tài khoản trực tuyến, ứng dụng VPN, phần mềm FTP, thông tin tài chính, dữ liệu từ các ứng dụng game, cookie Facebook, từ đó từ đó truy cập và tương tác với Facebook Ads Manager và Graph API nhằm thu thập dữ liệu quảng cáo, phục vụ các hoạt động bất hợp pháp.

2.6. Khuyến nghị

✓ **Kiểm tra và vá lỗi định kỳ:**

Ưu tiên vá các lỗ hổng trên Microsoft Exchange (ProxyLogon, ProxyNotShell), Oracle, Citrix Gateway, Zimbra, và Cisco ASA SSL VPN, những mục tiêu phổ biến của tin tặc.

Tăng cường kiểm tra các ứng dụng nội bộ và mã nguồn tự phát triển để phát hiện và sửa lỗi cho phép bypass authentication hoặc upload file tùy ý.

✓ **Giảm thiểu bề mặt tấn công:**

Hạn chế các thành phần facing ra Internet không cần thiết hoặc áp dụng các biện pháp bảo vệ như WAF (Web Application Firewall).

✓ **Tận dụng tối đa nguồn tin tình báo mạng**

NCS khuyến nghị các tổ chức, doanh nghiệp cập nhật các IoCs từ các chiến dịch tấn công, sự cố bảo mật, mã độc vào các giải pháp bảo mật nhằm nâng cao năng lực phòng thủ, giúp giám sát và phát hiện sớm các dấu hiệu, hành vi bất thường trên hệ thống.

3. Mối đe doạ về dữ liệu và tài khoản tại Việt Nam

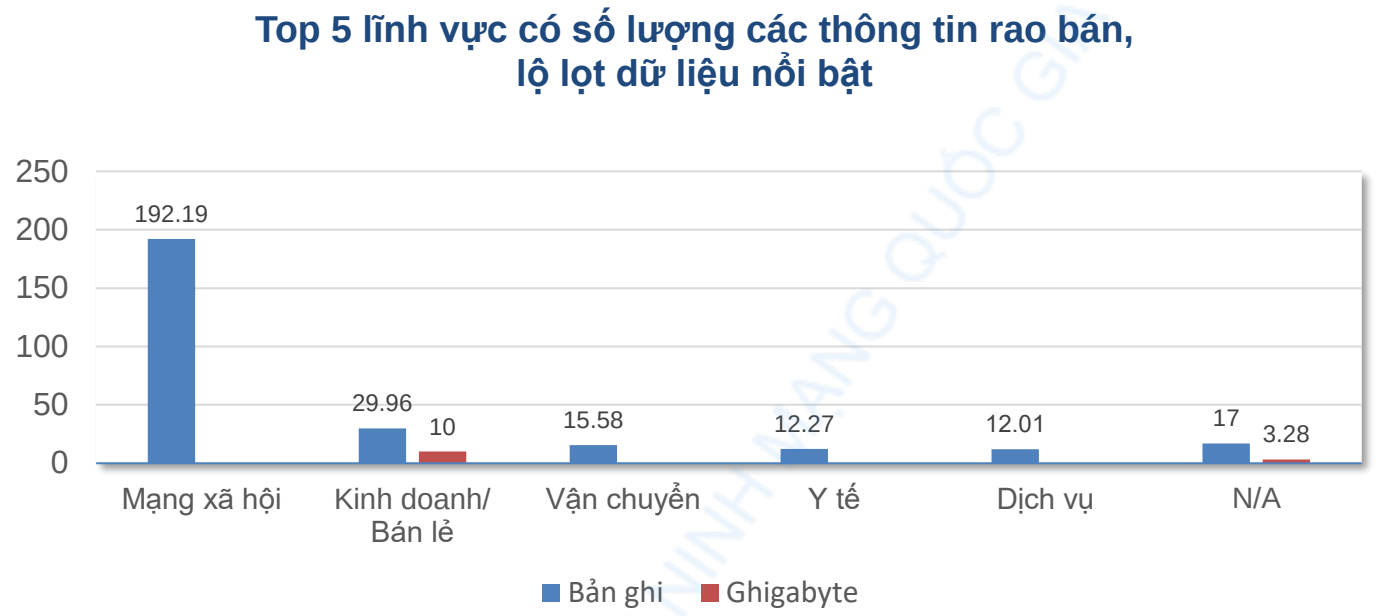
3.1. Thực trạng rao bán dữ liệu, lộ lọt tài khoản từ cá nhân đến tổ chức

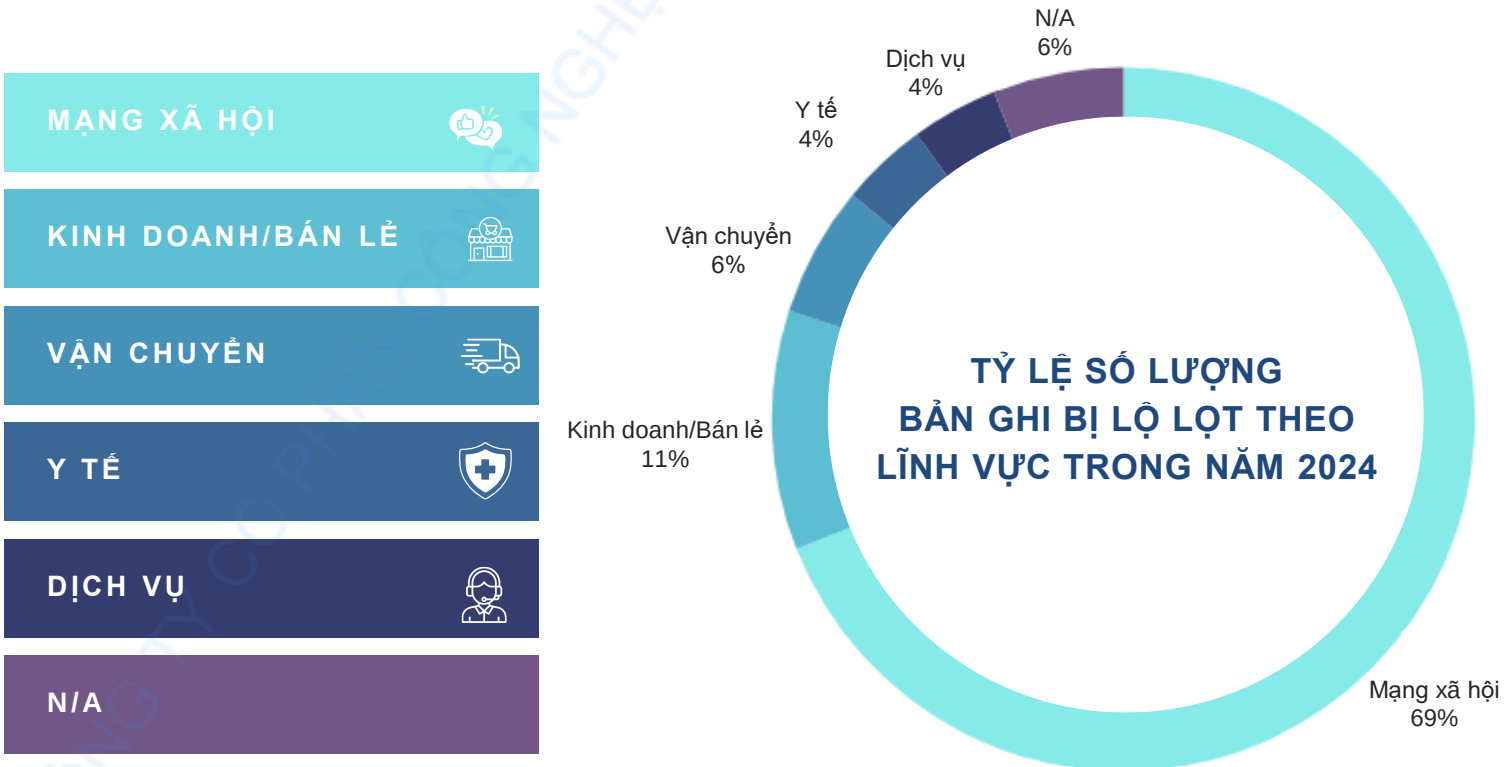
3.1.1. Tổng hợp thông tin, số lượng dữ liệu bị lộ lọt

Năm 2024, tình trạng lộ lọt và rao bán dữ liệu cá nhân, tổ chức tại Việt Nam tiếp tục diễn biến phức tạp. Hàng trăm triệu bản ghi, với dung lượng lên đến hàng chục GB, đã bị chia sẻ và rao bán công khai trên các chợ đen, diễn đàn ngầm và dark web. Các dữ liệu bị lộ lọt bao gồm thông tin cá nhân của người dùng, như tài khoản ngân hàng, hồ sơ eKYC, dữ liệu giao dịch, và cả dữ liệu nhạy cảm của các tổ chức, như thông tin truy cập hệ thống hay tài liệu nội bộ quan trọng.

STT	Lĩnh vực	Tổng số lượng dữ liệu rao bán/ lộ lọt	
		Bản ghi	GB
1	Mạng xã hội	192.192.603	N/A
2	Kinh doanh/ Bán lẻ	29.958.350	10GB
3	Vận chuyển	15.571.196	N/A
4	Y tế	12.076.315	N/A
5	Dịch vụ	12.009.083	N/A
6	Tài chính	10.007.276	N/A
7	Công nghệ	9.508.639	N/A
8	Thương mại điện tử	2.458.892	N/A
9	Thực phẩm	1.871.262	N/A
10	Du lịch	760.000	N/A
11	Truyền thông/Giải trí	577.912	N/A
12	Hàng không	50.000	N/A
13	Giáo dục/ Đào tạo	911.000	14GB
14	Chính phủ	6.000	N/A

3.1.2. Phân chia theo nhóm ngành





3.2. Nhận định và đánh giá từ chuyên gia

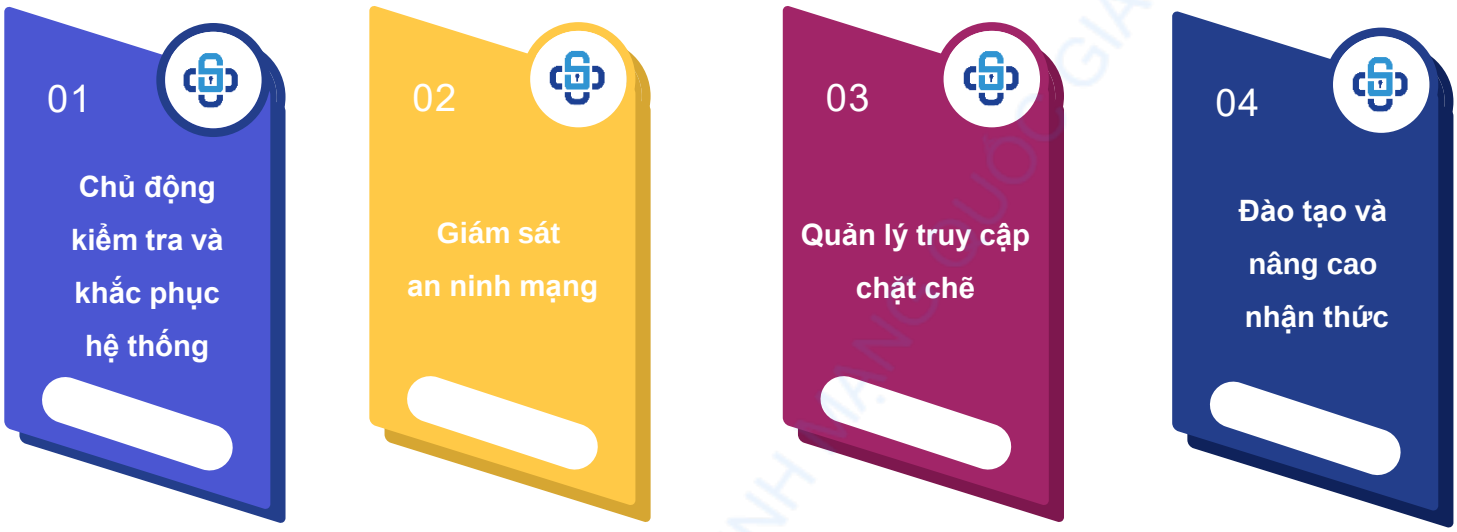
Một trong những nguyên nhân chính gây ra tình trạng này là **sự lây nhiễm mã độc từ các thiết bị cá nhân**. Đặc biệt, các loại mã độc đánh cắp thông tin (info-stealer malware) đã lợi dụng sự bất cẩn của người dùng khi tải phần mềm không rõ nguồn gốc, sử dụng phần mềm crack hoặc xử lý các email lạ. Những hành vi này tạo điều kiện cho mã độc xâm nhập và đánh cắp thông tin nhạy cảm qua trình duyệt hoặc các kênh khác.

Ngoài ra**, hệ thống bảo mật tại nhiều công ty, tổ chức vẫn còn tồn tại nhiều lỗ hổng và điểm yếu**. Những lỗ hổng này không chỉ khiến hệ thống dễ bị tấn công mà còn cho phép tin tặc truy cập và đánh cắp dữ liệu nội bộ quan trọng.

Tình trạng trên không chỉ gây tổn thất lớn về mặt dữ liệu mà còn đặt ra yêu cầu cấp bách trong việc nâng cao nhận thức về an ninh mạng, đồng thời tăng cường các biện pháp phòng ngừa để bảo vệ dữ liệu cá nhân và tổ chức.

3.3. Các giải pháp và khuyến nghị bảo mật

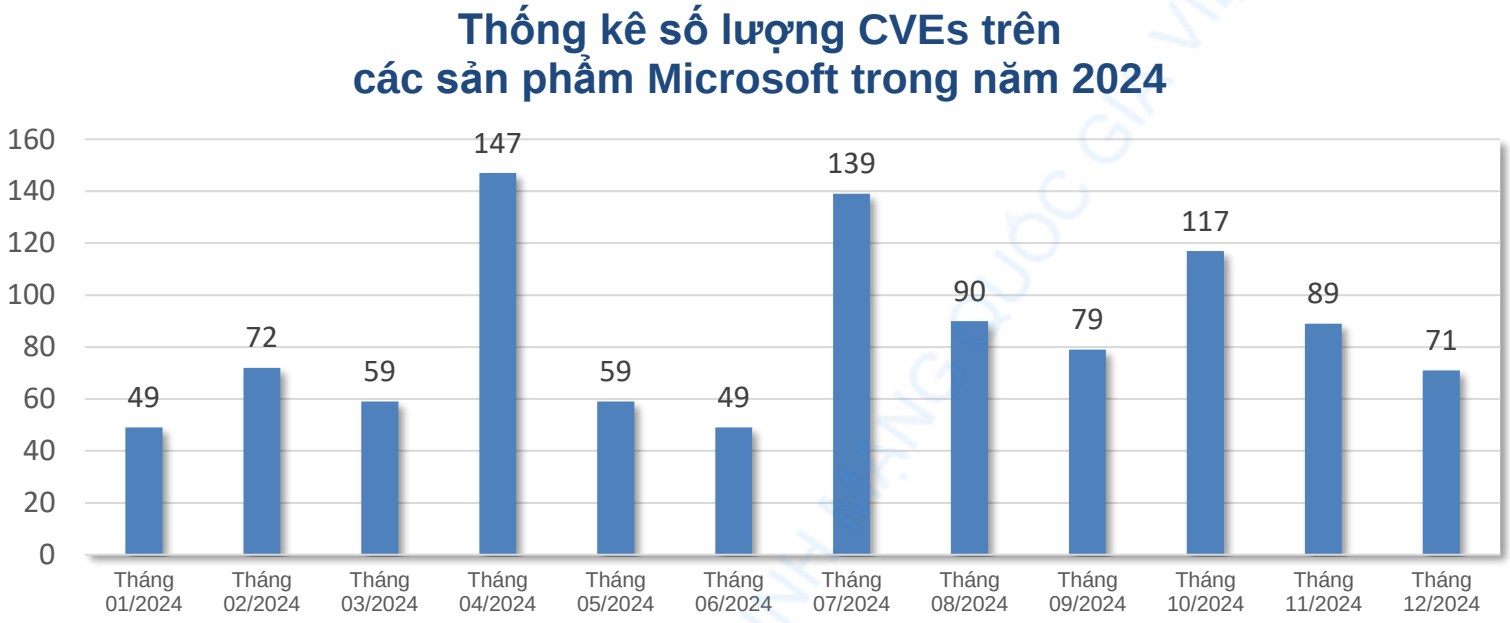
NCS đề xuất các giải pháp hiệu quả giúp doanh nghiệp và tổ chức bảo vệ tài khoản cũng như dữ liệu nhạy cảm trước các rủi ro tiềm ẩn:



- **Chủ động kiểm tra và khắc phục hệ thống:** Thường xuyên rà soát, đánh giá hệ thống để phát hiện kịp thời các điểm yếu, lỗ hổng. Lên kế hoạch xử lý và cập nhật các bản vá mới nhất cho các sản phẩm, giải pháp trong hệ thống.
- **Giám sát an ninh mạng:** Triển khai hệ thống giám sát để nhanh chóng phát hiện và ứng phó với các hành vi bất thường trong mạng lưới.
- **Quản lý truy cập chặt chẽ:** Áp dụng nguyên tắc quyền truy cập tối thiểu (least privilege) và sử dụng xác thực đa yếu tố (MFA) nhằm giảm nguy cơ xâm nhập trái phép.
- **Đào tạo và nâng cao nhận thức:** Tổ chức các buổi tập huấn định kỳ nhằm nâng cao nhận thức và kỹ năng bảo mật an ninh mạng cho toàn bộ nhân viên.

4. Lỗ hổng bảo mật

4.1. Tổng hợp các lỗ hổng bảo mật trên sản phẩm Microsoft

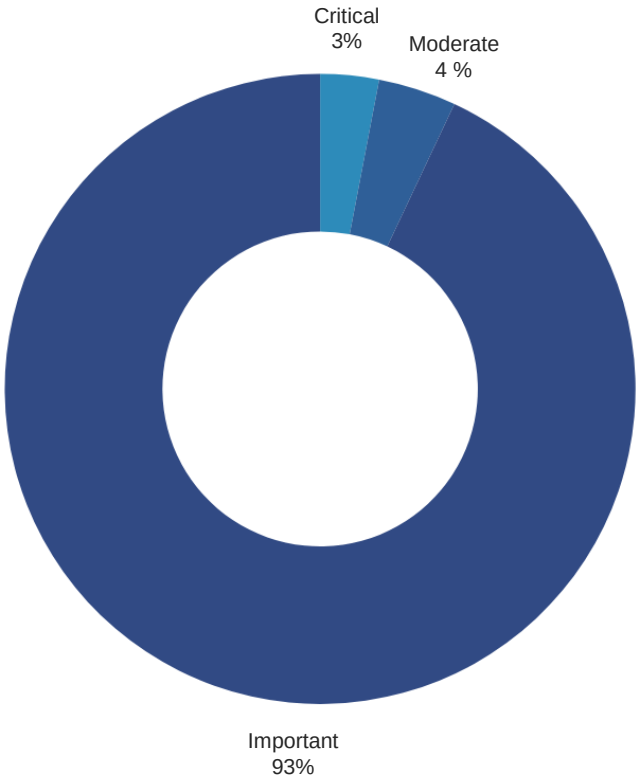


Trong năm 2024, Microsoft đã phát hành bản vá cho tổng cộng **1,020 lỗ hổng** trên nhiều sản phẩm quan trọng như Windows, Windows Components, Office, Office Components, Azure, .NET Framework, SQL Server, Hyper-V và nhiều sản phẩm khác.

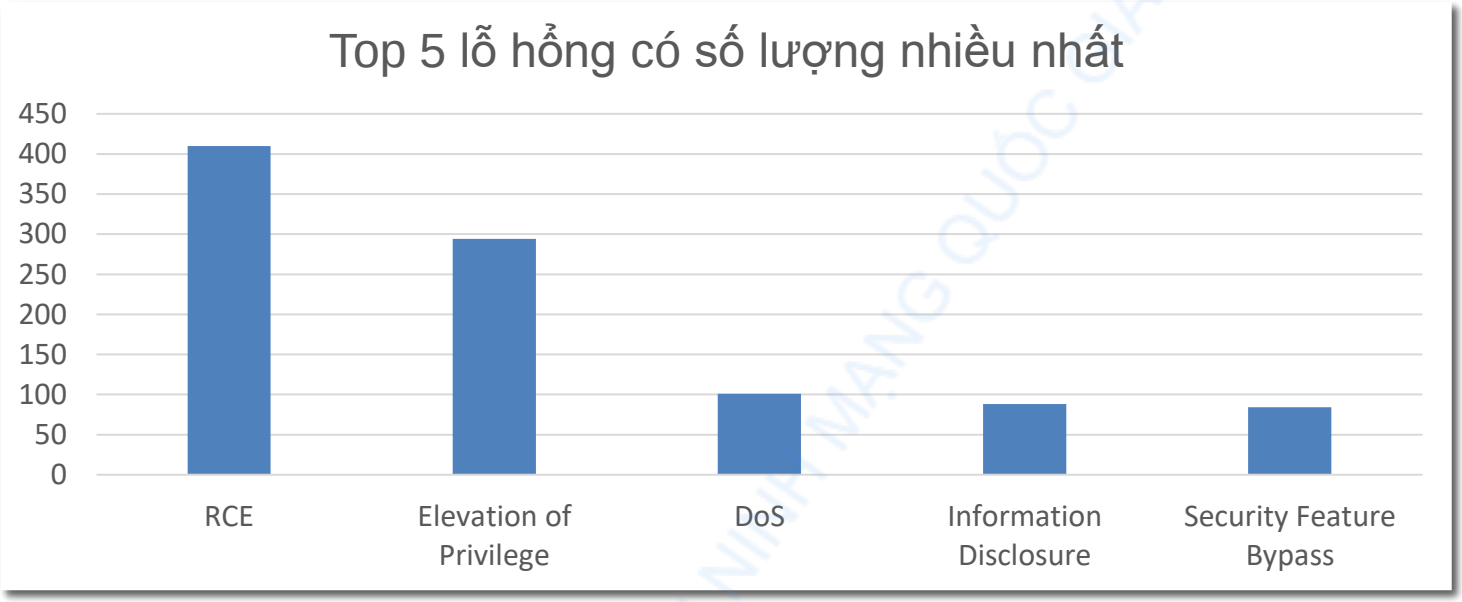
41 lỗ hổng được đánh giá ở mức độ **Moderate**.

951 lỗ hổng được đánh giá ở mức độ **Important**.

28 lỗ hổng được đánh giá ở mức độ **Critical**.



4.1. Tổng hợp các lỗ hổng bảo mật trên sản phẩm Microsoft



STT	Loại lỗ hổng	Số lượng
1	RCE	410
2	Elevation of Privilege	294
3	DoS	101
4	Information Disclosure	88
5	Security Feature Bypass	84

4.2. Tổng hợp các lỗ hổng bảo mật trên các sản phẩm khác

Trong năm 2024, NCS ghi nhận các lỗ hổng nổi bật trên các sản phẩm khác. Đây đều là các lỗ hổng trên các sản phẩm phổ biến được sử dụng trong môi trường doanh nghiệp.

- **Sản phẩm Apache** (Apache HTTP Server, Apache Struts) ghi nhận 3 lỗ hổng trong đó **2 lỗ hổng** đánh giá mức độ **Important** và **1 lỗ hổng** đánh giá mức độ **Critical**. Các lỗ hổng này bao gồm lỗ hổng cho phép tiết lộ các thông tin nhạy cảm, và lỗ hổng cho phép kẻ tấn công upload file độc hại từ đó thực thi mã từ xa.
- **Sản phẩm BIG-IP** ghi nhận **3 lỗ hổng được đánh giá mức độ High**. Trong đó 2 lỗ hổng cho phép kẻ tấn công thu thập các thông tin nhạy cảm, 1 lỗ hổng cho phép kẻ tấn công leo thang đặc quyền.

- **Sản phẩm Citrix** (Citrix NetScaler ADC and Gateway và Citrix Session Recording): ghi nhận **5 lỗ hổng** trong đó **2 lỗ hổng được đánh giá mức độ High và 3 lỗ hổng được đánh giá mức độ Medium.** Các lỗ hổng này chủ yếu là lỗ hổng cho phép kẻ tấn công thực thi mã từ xa và lỗ hổng leo thang đặc quyền trên hệ thống bị ảnh hưởng.
- **Sản phẩm Ivanti** (Ivanti Cloud Services Application, Ivanti Connect Secure, Ivanti Connect Secure & Policy Secure): **ghi nhận 8 lỗ hổng trong đó 6 lỗ hổng được đánh giá mức độ Critical, 2 lỗ hổng được đánh giá mức độ High**. Các lỗ hổng này chủ yếu là lỗ hổng cho phép kẻ tấn công thực thi mã từ xa trên hệ thống bị ảnh hưởng.
- **Sản phẩm Jenkins**: Bao gồm **2 lỗ hổng trong đó 1 lỗ hổng được đánh giá mức độ Critical, 1 lỗ hổng đánh giá mức độ Medium**. Cả hai lỗ hổng này đều là lỗ hổng cho phép kẻ tấn công thu thập các dữ liệu nhạy cảm.
- **Sản phẩm NetScaler** (NetScaler Console, NetScaler SDX, NetScaler Agent) bao gồm 2 lỗ hổng trong đó **1 lỗ hổng được đánh giá mức độ Critical, 1 lỗ hổng được đánh giá mức độ High.** Các lỗ hổng bao gồm lỗ hổng cho phép kẻ tấn công đọc và truy cập vào các dữ liệu nhạy cảm. Ngoài ra, tồn tại lỗ hổng từ chối dịch vụ, khai thác lỗ hổng yêu cầu kẻ tấn công có quyền truy cập vào địa chỉ IP của NetScaler Console, NetScaler Agent, NetScaler SDX (SVM).
- **Sản phẩm Palo Alto** (Palo Alto Networks GlobalProtect, PAN-OS, Palo Alto Networks Cortex XSOAR, Palo Alto Networks Expedition) **ghi nhận 10 lỗ hổng trong đó 1 lỗ hổng được đánh giá mức độ Critical, 3 lỗ hổng được đánh giá mức độ High và 6 lỗ hổng được đánh giá mức độ Medium.** Các lỗ hổng này chủ yếu là lỗ hổng cho phép kẻ tấn công leo thang đặc quyền, lỗ hổng thực thi mã từ xa (RCE), tấn công DOS và đọc file tùy ý.

- **Sản phẩm Splunk** (Splunk Enterprise và Splunk Secure Gateway) ghi nhận **3 lỗ hổng** được đánh giá mức độ High trong đó 2 lỗ hổng cho phép kẻ tấn công thực thi mã từ xa và 1 lỗ hổng cho phép đọc thông tin nhạy cảm trên hệ thống bị ảnh hưởng.
- **Sản phẩm Veeam Backup & Replication**: ghi nhận **8 lỗ hổng trong đó 5 lỗ hổng đánh giá mức độ Critical và 3 lỗ hổng được đánh giá mức độ High**. Các lỗ hổng này chủ yếu là lỗ hổng cho phép kẻ tấn công thực thi mã từ xa, lỗ hổng vượt qua cơ chế xác thực, lỗ hổng lộ lọt thông tin nhạy cảm...
- **Sản phẩm VMware** (VMware SD-WAN Edge và VMware vCenter Server): **ghi nhận 9 lỗ hổng trong đó 4 lỗ hổng mức độ Critical, 3 lỗ hổng được đánh giá mức độ High, 1 lỗ hổng đánh giá mức độ Important và 1 lỗ hổng đánh giá mức độ Moderate**. Các lỗ hổng này chủ yếu là các lỗ hổng cho phép kẻ tấn công thực thi mã từ xa, lỗ hổng leo thang đặc quyền, lỗ hổng cho phép thực thi các đoạn mã độc hại, và lỗ hổng bỏ qua xác thực ...
- **Sản phẩm Zabbix: ghi nhận 5 lỗ hổng trong đó 4 lỗ hổng được đánh giá mức độ Critical, 1 lỗ hổng được đánh giá mức độ High**. Các lỗ hổng này bao gồm lỗ hổng cho phép kẻ tấn công leo thang đăc quyền, lỗ hổng thực thi mã **ghi nhận 1 lỗ hổng được đánh giá với mức độ Critical**từ xa trên hệ thống bị ảnh hưởng.
- **Sản phẩm SonicOS: ghi nhận 1 lỗ hổng được đánh giá với mức độ Critical**. Lỗ hổng cho phép kẻ tấn công truy cập trái phép vào các tài nguyên của hệ thống, có thể dẫn đến tình trạng crash firewall.
- **Sản phẩm SolarWinds** (SolarWinds Access Rights Manager (ARM), SolarWinds Platform) ghi nhận **10 lỗ hổng trong đó 1 lỗ hổng được đánh giá với mức độ Medium và 9 lỗ hổng được đánh giá mức độ Critical**. Các lỗ hổng bao gồm lỗ hổng cho phép kẻ tấn công thu thập thông tin nhạy cảm, lỗ hổng thực thi mã từ xa, lỗ hổng cho phép kẻ tấn công đọc và xóa file tùy ý, lỗ hổng Race Condition.

- **Sản phẩm Firefox:** ghi nhận **1 lỗ hổng được đánh giá mức độ Critical**. Lỗ hổng này cho phép kẻ tấn công thực thi mã từ xa và sandbox escape ảnh hưởng đến Firefox thấp hơn phiên bản 124.0.1.
- **Sản phẩm Check Point Security Gateways** ghi nhận **1 lỗ hổng được đánh giá mức độ High.** Đây là lỗ hổng lộ lọt thông tin trong Check Point Security Gateways.
- **Sản phẩm ManaEngine OpManager: ghi nhận 1 lỗ hổng được đánh giá mức độ High**. Đây là lỗ hổng Path Traversal trong tính năng UploadMib của ManaEngine OpManager
- **Sản phẩm Oracle WebLogic: ghi nhận 1 lỗ hổng được đánh giá mức độ Critical**. Lỗ hổng này cho phép kẻ tấn công không xác thực chiếm được quyền kiểm soát máy chủ.
- **Sản phẩm Confluence Data Center and Server**: Ghi nhận **1 lỗ hổng** được đánh giá mức độ **High**. Lỗ hổng này cho phép kẻ tấn công thực thi các đoạn mã tùy ý.

4.3. Các lỗ hổng bảo mật nổi bật 2024

NCS ghi nhận các lỗ hổng mới được công bố trong năm 2024, đồng thời nhận diện những trường hợp các lỗ hổng này bị khai thác trong các chiến dịch tấn công thực tế. Các nhóm tấn công đã tận dụng những lỗ hổng này để giành quyền truy cập ban đầu vào hệ thống của mục tiêu, mở đường cho các hoạt động tấn công phức tạp tiếp theo.

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm bị ảnh hưởng	Mức độ
1	CVE-2023-46805	Authentication Bypass	Bypass authen cho phép kẻ tấn công truy cập vào các tài nguyên bị hạn chế	Ivanti Connect Secure VPN	High
2	CVE-2024-21887	Command Injection	Tồn tại lỗ hổng command injection cho phép kẻ tấn công thực đi đoạn code độc hại. Được kết hợp với lỗ hổng CVE-2023-46805 tạo thành bug chain nhằm triển khai đa dạng các loại webshell.	Ivanti Connect Secure VPN	Critical
3	CVE-2024-21413	Microsoft Outlook Remote Code Execution	Tồn tại lỗ hổng RCE trong Microsoft Outlook, khai thác thành công cho phép đánh cắp thông tin đăng nhập Windows NTLM và thực thi mã tùy ý mà không cần sự tương tác của người dùng.	Microsoft	Critical

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm	Mức độ
4	CVE-2024-21412	Internet Shortcut Files Security Feature Bypass Vulnerability	Tồn tại lỗ hổng vượt qua cơ chế bảo mật trong Microsoft Defender SmartScreen nhằm triển khai mã độc	Microsoft	High
5	CVE-2024-21410	Microsoft Exchange Server Elevation of Privilege Vulnerability	Tồn tại lỗ hổng leo thang đặc quyền trong Microsoft Exchange Server	Microsoft Exchange Server	Critical
6	CVE-2024-21413	Microsoft Outlook Remote Code Execution	Tồn tại lỗ hổng RCE trong Microsoft Outlook, khai thác thành công cho phép đánh cắp thông tin đăng nhập Windows NTLM và thực thi mã tùy ý mà không cần sự tương tác của người dùng.	Microsoft	Critical

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm	Mức độ
7	CVE-2024-3400	Arbitrary File Creation Leads to OS Command Injection Vulnerability	Tồn tại lỗ hổng command inject cho phép kẻ tấn công thực thi đoạn mã tùy ý với đặc quyền root	Palo Alto Networks PAN-OS	Critical
8	CVE-2024-20359	Local Code Execution Vulnerability	Tồn tại lỗ hổng cho phép kẻ tấn công được xác thực thực thi mã từ xa với đặc quyền root.	Cisco ASA Software và FTD Software	High
9	CVE-2024-4671	Use after free in Visuals	Tồn tại lỗ use-after-free trong thần Visuals của Google Chrome cho phép kẻ tấn công escape sandbox	Google Chrome	Critical
10	CVE-2024-4947/ CVE-2024-5274	Type confusion	Type confusion trong V8 engine cho phép thực thi mã	Google Chrome	High

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm	Mức độ
11	CVE-2024-4761	Out-of-bounds write	Out-of-bounds write trong V8 engine	Google Chrome	High
12	CVE-2024-30040	Windows MSHTML Platform Security Feature Bypass Vulnerability	Lỗ hổng vượt qua các cơ chế bảo mật OLE mitigations trong Microsoft 365 và Microsoft Office	Microsoft	Important
13	CVE-2024-30051	Windows DWM Core Library Elevation of Privilege Vulnerability	Khai thác thành công cho phép thực thi dưới đặc quyền hệ thống	Microsoft	Important
14	CVE-2024-4577	Remote Code Execution	Tồn tại lỗ hổng cho phép kẻ tấn công không cần xác thực thực thi đoạn mã tùy ý	PHP (cài đặt trên hệ điều hành Windows sử dụng CGI mode)	High

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm	Mức độ
15	CVE-2024-6387	OpenSSH Server Remote Unauthenticated Code Execution vulnerability	Tồn tại lỗ hổng race-condition trong ssh cho phép kẻ tấn công thực thi đoạn mã tùy ý với quyền root	OpenSSH	High
16	CVE-2024-38213	Windows Mark of the Web Security Feature Bypass Vulnerability	Tồn tại lỗ hổng bypass cơ chế bảo mật trong SmartScreen	Microsoft	Moderate
17	CVE-2024-28986	Java Deserialization Remote Code Execution	Tồn tại lỗ hổng cho phép kẻ tấn công thực thi mã từ xa	SolarWinds Web Help Desk	Critical
18	CVE-2024-4577	Remote Code Execution	Tồn tại lỗ hổng cho phép kẻ tấn công không cần xác thực thực thi đoạn mã tùy ý	PHP (cài đặt trên hệ điều hành Windows sử dụng CGI mode)	High
19	CVE-2024-45519	Remote Code Execution	Tồn tại lỗ hổng cho phép kẻ tấn công không cần xác thực thực thi mã từ xa	Zimbra Collaboration	Critical

STT	Mã CVE	Tên lỗ hổng	Thông tin chung	Sản phẩm	Mức độ
20	CVE-2024-45844	Privilege escalation in BIG-IP monitor	Tồn tịa lỗ hổng cho phép kẻ tấn công nâng cao đặc quyền hoặc sửa đổi cấu hình	F5	High
21	CVE-2024-0012	Authentication Bypass in the Management Web Interface	Tồn tại lỗ hổng bỏ qua xác thực trong Palo Alto Networks PAN-OS cho phép kẻ tấn công không cần xác thực có quyền truy cập vào Management Web Interface, nhằm giành đặc quyền administrator từ đó thực hiện các hoạt động độc hại khác	Palo Alto Networks PAN-OS	Critical
22	CVE-2024-9474	Privilege Escalation (PE) Vulnerability in the Web Management Interface	Tồn tại lỗ hổng leo thang đặc quyền trong Palo Alto Networks PAN-OS cho phép kẻ tấn công thực hiện các hoạt động độc hại với đặc quyền root.	Palo Alto Networks PAN-OS	Medium

4.4. Khuyến nghị

NCS khuyến nghị các tổ chức, doanh nghiệp thực hiện rà soát và lên kế hoạch cập nhật bản vá cho các lỗ hổng bảo mật theo hướng dẫn của hãng để đảm bảo an toàn an ninh thông tin hệ thống.

Dự đoán
Xu hướng 2025

IV. DỰ ĐOÁN XU HƯỚNG 2025

1. Dự báo về các mối đe doạ sắp tới

Dựa trên các sự kiện an ninh mạng và xu hướng công nghệ diễn ra trên toàn cầu, chúng tôi đã phân tích và đưa ra nhận định về các hệ thống có khả năng trở thành mục tiêu "ưa thích" của hacker tại Việt Nam trong vài năm tới:

Hệ thống đám mây: Vùng đất hứa của tin tặc

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ, nhiều tổ chức và doanh nghiệp tại Việt Nam đã dịch chuyển sang sử dụng dịch vụ đám mây như AWS, Microsoft Azure hoặc Google Cloud. Tuy nhiên, việc thiếu cấu hình bảo mật phù hợp đã khiến các dịch vụ này trở thành mục tiêu lý tưởng. Vụ việc xảy ra trên Microsoft Azure vào tháng 9/2023 là minh chứng điển hình. Microsoft đã vô tình sử dụng một token SAS (Shared Access Signature) không giới hạn để chia sẻ dữ liệu AI mã nguồn mở. Sai lầm này dẫn đến việc lộ 38 terabyte dữ liệu, bao gồm cả khóa mã hóa và mật khẩu.

Cách thức tin tặc khai thác:

- Quét tìm cấu hình sai: Tin tặc sử dụng các công cụ tự động như Shodan hoặc Censys để tìm kiếm các dịch vụ đám mây với cấu hình mở hoặc thiếu mã hóa.
- Khai thác quyền truy cập không giới hạn: Khi phát hiện các quyền truy cập mặc định hoặc không được kiểm soát chặt chẽ, tin tặc dễ dàng truy cập trái phép để đánh cắp dữ liệu hoặc chiếm quyền điều khiển tài nguyên.

Ngoài ra, một hình thức xâm nhập nguy hiểm hơn của hacker vào các hệ thống Cloud đó là đánh cắp token và sử dụng nó làm "chìa khoá" đi vào bên trong. Token truy cập vốn là công cụ để xác thực người dùng và duy trì các phiên làm việc trên dịch vụ đám mây. Vụ tấn công Storm-0558 vào tháng 7/2023 là một minh chứng điển hình. Nhóm tin tặc Trung Quốc đã đánh cắp khóa ký tên MSA (Microsoft Signing Key) từ môi trường gỡ lỗi của Microsoft. Sau đó, chúng tạo các token giả mạo, cho phép truy cập trái phép vào email và tài khoản đám mây của hơn 25 tổ chức, bao gồm cả các cơ quan chính phủ Hoa Kỳ. Một ví dụ khác về việc đánh cắp token xảy ra trong vụ tấn công nhắm vào công ty quản lý danh tính Okta vào tháng 10 năm 2023. Tin tặc đã sử dụng thông tin đăng nhập bị đánh cắp để truy cập vào hệ thống hỗ trợ khách hàng của Okta. Từ đó, chúng chiếm dụng các tệp HTTP Archive (HAR) do khách hàng tải lên, chứa thông tin quan trọng như cookie và token phiên làm việc. Các token này sau đó được sử dụng để chiếm quyền kiểm soát hệ thống và truy cập trái phép vào các tài khoản của khách hàng.

Cách thức tin tặc khai thác:

- Sử dụng token từ phiên làm việc cũ: Tin tặc khôi phục token từ các tệp ghi nhật ký hoặc bộ nhớ hệ thống chưa được xóa sạch. Nếu hệ thống không hủy token sau khi phiên làm việc kết thúc, tin tặc có thể tái sử dụng để truy cập trái phép.
- Lừa đảo lấy mã xác thực (Social Engineering): Tin tặc giả danh nhân viên hỗ trợ kỹ thuật để yêu cầu mã xác thực đa yếu tố (MFA) hoặc mã truy cập từ người dùng.

1.2. Tấn công chuỗi cung ứng: Thách thức nghiêm trọng đối với an ninh mạng toàn cầu

Tấn công chuỗi cung ứng đã và đang trở thành một trong những mối đe dọa lớn nhất đối với an ninh mạng toàn cầu**. Trên thực tế, đội ngũ Redteam của NCS từng triển khai thử nghiệm PoC** hình thức này tại một số tổ chức ở Việt Nam, minh chứng rõ nét về mức độ nguy hiểm. **Chỉ trong vòng một đến hai tuần, đội ngũ của chúng tôi đã có thể xâm nhập thành công vào hạ tầng khách hàng – nhanh hơn đáng kể so với thời gian một đến ba tháng của các cuộc tấn công Redteam truyền thống.**

Khác với những phương thức tấn công trực tiếp, hình thức này tập trung khai thác các nhà cung cấp dịch vụ hoặc đối tác trong chuỗi cung ứng để tiếp cận hệ thống mục tiêu. Một ví dụ điển hình là vụ tấn công vào ứng dụng VoIP 3CX vào năm 2023. Cả phiên bản Windows và macOS của 3CXDesktopApp – một sản phẩm của 3CX Communications – đã bị tấn công, dẫn đến việc phát tán mã độc trên quy mô lớn trong chiến dịch mang tên "SmoothOperator." Chiến dịch này đã ảnh hưởng đến hơn 600.000 công ty trên toàn cầu, và được liên kết với nhóm Lazarus của Triều Tiên (CVE-2023-29059).

Không chỉ các ứng dụng thương mại, chuỗi cung ứng phần mềm nguồn mở cũng là mục tiêu dễ bị tổn thương. Năm 2024, công cụ nén dữ liệu XZ Utils đã trở thành nạn nhân khi tin tặc thâm nhập dự án, chèn backdoor vào mã nguồn chính thức. Sau khi phát hành, backdoor này cho phép kiểm soát từ xa nhiều hệ thống, bao gồm OpenSSH. Lỗ hổng này, được mã hóa CVE-2024-30942, được đánh giá ở mức nghiêm trọng nhất (mức 10) bởi NIST.

Những cuộc tấn công chuỗi cung ứng thường bắt đầu từ việc khai thác lỗ hổng bảo mật hoặc các kỹ thuật lừa đảo (phishing) nhằm xâm nhập nhà cung cấp. Sau đó, tin tặc chèn mã độc hoặc chỉnh sửa mã nguồn, gây ra tác động dây chuyền với hậu quả khôn lường trên quy mô lớn. Để đối phó, các tổ chức cần cảnh giác hơn trong việc lựa chọn và giám sát đối tác cung cấp dịch vụ, nhằm bảo vệ toàn diện hệ thống của mình.

1.3.Tấn công API: Nguy cơ tiềm ẩn trong an ninh mạng hiện đại

API (Application Programming Interface) đóng vai trò quan trọng trong việc kết nối các hệ thống, ứng dụng, và dữ liệu. Một thống kê gần đây cho thấy trên 80% lưu lượng Internet toàn cầu được khởi tạo bởi các cuộc gọi API. Năm 2024, nhiều cuộc tấn công API đã gây ra những hậu quả nghiêm trọng, làm nổi bật mức độ nguy hiểm của loại hình tấn công này. Một lỗ hổng nghiêm trọng trong API của Dell đã bị tin tặc khai thác qua cổng đối tác (Partner Portal). Tin tặc lợi dụng lỗi logic trong API, cho phép chúng vượt qua cơ chế xác thực và truy cập trực tiếp vào dữ liệu của khách hàng. Kết quả là hơn 49 triệu hồ sơ khách hàng bị rò rỉ, bao gồm thông tin cá nhân, lịch sử mua hàng, và chi tiết thanh toán.

Phương pháp tấn công này không cần đến kỹ thuật phức tạp, nhưng việc thiếu giám sát và kiểm tra logic kinh doanh của API đã tạo cơ hội cho tin tặc khai thác hiệu quả. Vụ việc làm tổn hại nghiêm trọng đến uy tín của Dell, đồng thời buộc công ty phải chi hàng triệu USD để xử lý hậu quả và cải thiện hệ thống

Trong một sự cố khác, tin tặc đã sử dụng các khóa API bị lộ để truy cập vào môi trường sản xuất của Dropbox. Chúng khai thác hệ thống để thu thập dữ liệu khách hàng, bao gồm thông tin xác thực đa yếu tố (MFA). Bằng cách tận dụng các khóa API không được bảo vệ, tin tặc không chỉ xâm nhập hệ thống mà còn duy trì quyền truy cập trong thời gian dài mà không bị phát hiện. Sự cố này không chỉ làm lộ dữ liệu của hàng triệu người dùng mà còn gây ra lo ngại về khả năng bảo vệ dữ liệu trong môi trường đám mây của Dropbox

2. Những công nghệ và dịch vụ phòng vệ mới

Trước sự gia tăng của các mối đe dọa ngày càng tinh vi và khó dự đoán, việc triển khai các giải pháp và dịch vụ bảo mật hiệu quả trở thành yêu cầu cấp thiết. Dưới đây là một số gợi ý của NCS giúp các tổ chức lựa chọn giải pháp phù hợp với nhu cầu và đặc thù của mình:

2.1. Sự quan trọng của việc bảo vệ "vòng ngoài" với Attack surface managment

Trong ba năm qua, các thương vụ lớn như Google mua lại Mandiant, Mastercard thâu tóm Recorded Future, đây đều là những hãng bảo mật nổi tiếng với nền tảng tình báo mạng, đã khẳng định rằng bảo mật hiện đại cần một góc nhìn toàn diện về bề mặt tấn công – bao gồm đám mây, IoT, dark web và rủi ro từ bên thứ ba.

Các công ty CTI hàng đầu đang chuyển đổi để cung cấp giải pháp Quản lý Bề mặt Tấn công (ASM), giúp tổ chức nhìn nhận hệ thống giống như cách kẻ tấn công quan sát. Với khả năng này, tổ chức có thể xây dựng chiến lược giảm thiểu rủi ro hiệu quả hơn. ASM đang phát triển mạnh mẽ với tốc độ tăng trưởng dự báo 30% CAGR đến năm 2030, nhanh gấp đôi thị trường bảo mật chung.

ASM không chỉ hỗ trợ phát hiện và khắc phục lỗ hổng trong hệ thống mà còn đóng vai trò quan trọng trong quản lý rủi ro chuỗi cung ứng – một lĩnh vực mà nhiều tổ chức vẫn chưa đầu tư đủ. Với khả năng giám sát rủi ro từ đối tác và nhà cung cấp, ASM giảm nguy cơ tấn công qua các tài sản không thuộc quyền quản lý trực tiếp. Điều này đặc biệt quan trọng khi tấn công chuỗi cung ứng đang ngày càng gia tăng, nhắm vào các đối tác để xâm nhập hệ thống mục tiêu.

Ngoài ra, ASM còn tích hợp Cloud Security Posture Management (CSPM), đảm bảo các hệ thống đám mây được thiết lập đúng chuẩn bảo mật. Tính năng này giúp phát hiện lỗi cấu hình, lỗ hổng API và các quyền truy cập không hợp lệ, bảo vệ dữ liệu quan trọng trong môi trường số hóa.

ASM không chỉ là giải pháp công nghệ mà còn là công cụ chiến lược giúp tổ chức chủ động kiểm soát an ninh, bảo vệ toàn diện trước các mối đe dọa phức tạp của thế giới số.

2.2. Giải pháp bảo vệ tiết kiệm chi phí cho các doanh nghiệp vừa và nhỏ - MDR

Trước yêu cầu ngày càng nghiêm ngặt về bảo vệ dữ liệu cá nhân tại Việt Nam, các doanh nghiệp lưu trữ và xử lý dữ liệu người dùng buộc phải triển khai những phương án an ninh mạng bảo vệ. Tuy nhiên, đối với các doanh nghiệp vừa và nhỏ (SMB), nguồn lực hạn chế về tài chính và nhân sự chuyên môn khiến việc xây dựng hệ thống bảo mật nội bộ, như Trung tâm Điều hành An ninh (SOC), trở thành thách thức lớn.

SOC được ví như một giải pháp "may đo thủ công" dành riêng cho các tổ chức lớn, yêu cầu đầu tư lớn vào hạ tầng công nghệ và nhân sự vận hành, điều mà nhiều SMB không thể đáp ứng. Trong khi đó, MDR nổi lên như một giải pháp hiện đại, hiệu quả và tối ưu chi phí. Tựa như dịch vụ "sản xuất hàng loạt" dựa trên công nghệ tiên tiến, MDR tận dụng nền tảng XDR (Extended Detection and Response) để cung cấp khả năng giám sát, phát hiện và phản ứng với các mối đe dọa 24/7, phù hợp với nhu cầu của các SMB.

MDR không chỉ giúp doanh nghiệp giảm thiểu chi phí mà còn mang lại những lợi ích vượt trội, bao gồm:

- Giám sát liên tục: Kịp thời phát hiện và xử lý các nguy cơ tiềm tàng.
- Chuyên gia bảo mật hỗ trợ: Tăng cường khả năng phòng thủ trước các cuộc tấn công mạng tinh vi.
- Tuân thủ quy định bảo mật: Đáp ứng tiêu chuẩn trong nước và quốc tế, củng cố niềm tin của khách hàng và đối tác.

Để tận dụng tối đa lợi ích từ MDR, doanh nghiệp cần cân nhắc kỹ lưỡng khi lựa chọn nhà cung cấp dịch vụ. Một nhà cung cấp đáng tin cậy phải có kinh nghiệm thực tiễn trong việc tích hợp và tối ưu các giải pháp XDR, cùng với khả năng hỗ trợ 24/7.

Managed Detection and Response không chỉ là giải pháp bảo mật đơn thuần, mà còn là chiến lược bảo vệ toàn diện, giúp các doanh nghiệp vừa và nhỏ tối ưu hóa nguồn lực, sẵn sàng đối mặt với các thách thức an ninh mạng trong thời đại số hóa.

2.3. Dịch vụ bảo mật cho Điện toán đám mây

Trong thời đại chuyển đổi số, điện toán đám mây (Cloud) đã trở thành yếu tố cốt lõi, hỗ trợ doanh nghiệp Việt Nam quản lý và vận hành dữ liệu hiệu quả. Tuy nhiên, sự phát triển nhanh chóng của Cloud kéo theo các mối đe dọa an ninh mạng ngày càng phức tạp, đòi hỏi các dịch vụ bảo mật chuyên biệt nhằm đảm bảo an toàn thông tin.

Các dịch vụ bảo mật Cloud quan trọng

Để bảo vệ dữ liệu và hệ thống, các dịch vụ bảo mật Cloud sau đây đang đóng vai trò thiết yếu:

- **Di trú lên Cloud an toàn**: Hỗ trợ doanh nghiệp chuyển đổi dữ liệu và ứng dụng lên Cloud với hiệu năng tối ưu, đồng thời đảm bảo tuân thủ các tiêu chuẩn bảo mật.
- **Audit cấu hình Cloud**: Đánh giá các thiết lập bảo mật như xác thực, quyền truy cập, cấu hình mạng, đảm bảo hạ tầng Cloud an toàn và chuẩn hóa.
- **Giám sát an ninh mạng 24/7**: Theo dõi liên tục để phát hiện và ngăn chặn các hành vi tấn công, đảm bảo hệ thống vận hành ổn định.
- **Kiểm thử bảo mật Cloud**: Tập trung vào bảo mật container, chức năng không máy chủ, và quản lý mã hóa để bảo vệ toàn diện các tài nguyên đám mây.
- **Tuân thủ rủi ro và tiêu chuẩn**: Đảm bảo hệ thống phù hợp với các quy định quốc tế như GDPR, ISO 27001 và các chuẩn trong nước.
- **Đào tạo nhận thức an ninh mạng**: Trang bị kỹ năng bảo mật cho nhân sự, giảm thiểu nguy cơ từ yếu tố con người.

Lựa chọn nhà cung cấp dịch vụ bảo mật Cloud

Việc hợp tác với nhà cung cấp dịch vụ bảo mật Cloud chuyên nghiệp giúp doanh nghiệp không chỉ bảo vệ tài sản kỹ thuật số mà còn tăng cường niềm tin với khách hàng và đối tác. Các dịch vụ bảo mật Cloud không chỉ là lớp phòng vệ mà còn là chiến lược dài hạn, đảm bảo sự phát triển bền vững trong một thế giới số hóa nhiều rủi ro.

NCS
PROTECT YOUR SUCCESS

CÔNG TY CỔ PHẦN CÔNG NGHỆ AN NINH MẠNG QUỐC GIA VIỆT NAM

Điện thoại: 024 85 888 000

Email: info@ncsgroup.vn

Trụ sở: Tràng An Complex, Số 1 Phùng Chí Kiên, Nghĩa Đô, Cầu Giấy, Hà Nội

Văn phòng TP.Hồ Chí Minh: 131 Trần Huy Liệu, Phường 8, Quận Phú Nhuận, Thành phố Hồ Chí Minh

Văn phòng Singapore: Work Central Offices Pte Ltd - 190 Clemenceau Ave, #06-01, Singapore, 239924