NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 24 (10/06/2024 – 16/06/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Trung Quốc "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam.

- **Cảnh báo:** Sleepy Pickle: Mối đe dọa mới đối với các mô hình Machine Learning.

- **Thông tin:** Hệ thống công nghệ thông tin của Bưu điện Việt Nam đã hoạt động trở lại.

2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 814** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Trung Quốc "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam"

Gần đây, các chuyên gia bảo mật đã phát hiện một chiến dịch gián điệp mạng tinh vi của nhóm APT Mustang Panda nhằm vào nhiều tổ chức tại Việt Nam. Nhóm APT này có nguồn gốc từ Trung Quốc, nổi tiếng với các kỹ thuật xâm nhập phức tạp nhằm tấn công vào các mạng lưới của chính phủ, tổ chức phi lợi nhuận và các cơ sở giáo dục.

Mustang Panda thường thực hiện các chiến dịch tấn công gián điệp phục vụ lợi ích của chính phủ Trung Quốc, không chỉ nhắm đến Việt Nam mà còn tấn công Hoa Kỳ, Châu Âu, và nhiều nước Châu Á như Mông Cổ, Myanmar, và Pakistan. Các cuộc tấn công của nhóm này thường có độ chính xác cao, duy trì sự xâm nhập lâu dài trong hệ thống mục tiêu khiến cho các cuộc tấn công của họ trở nên cực kỳ nguy hiểm.

Trong chiến dịch gần đây, Mustang Panda đã sử dụng các mồi nhử liên quan đến lĩnh vực giáo dục và thuế, đồng thời, tận dụng các công cụ hợp pháp như "forfiles.exe" để thực thi các file độc hại từ máy chủ C&C. Nhóm này cũng khai thác PowerShell, VBScript và các file batch để triển khai các hoạt động này, cho thấy sự thành thạo trong việc né tránh các biện pháp bảo mật.

Một điểm nổi bật trong cách thức hoạt động của Mustang Panda là việc nhóm này nhúng các file mồi nhử vào trong các file shortcut LNK độc hại. Chiến thuật này không chỉ làm tăng kích thước payload, mà còn giảm khả năng bị phát hiện bởi các biện pháp bảo mật. Họ đạt được điều này bằng cách trộn lẫn các thành phần của file mồi nhử trực tiếp vào trong file gốc, khiến việc truy quét trở nên khó khăn hơn.

Sự tinh vi của Mustang Panda được thể hiện qua việc sử dụng kỹ thuật DLL sideloading để thực thi mã độc trên thiết bị, giúp duy trì kết nối và mở đường cho các hoạt động độc hại tiếp theo.

Trong chiến dịch gần đây nhắm vào Việt Nam, nhóm này đã sử dụng các file mồi nhử liên quan đến thuế vào tháng 05/2024 và trước đó là các file về giáo dục vào tháng 04/2024.

Nguồn: https://thecyberexpress.com/mustang-panda-target-vietnamese-firms/

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Trung Quốc "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam"

Cả hai chiến dịch đều bắt đầu từ email lừa đảo có đính kèm file độc hại, nhằm lừa người dùng mở và kích hoạt mã độc. Phân tích chuyên sâu về chiến dịch của Mustang Panda vào tháng 05/2024 cho thấy nhóm này đã sử dụng kỹ thuật đặt hai đuôi file để che giấu bản chất độc hại của chúng. Payload được ngụy trang dưới dạng file PDF, nhưng thực chất chứa các lệnh PowerShell để tải xuống và thực thi mã độc từ máy chủ từ xa.

Kỹ thuật DLL sideloading đã được Mustang Panda áp dụng để ẩn các hành vi độc hại vào trong tiến trình tuần tự của hệ thống, từ đó giảm thiểu nguy cơ bị phát hiện và duy trì kết nối đến thiết bị bị ảnh hưởng. Chiến dịch tấn công này một lần nữa làm rõ mối đe dọa ngày càng gia tăng từ các nhóm sở hữu kỹ thuật tấn công tinh vi. Bằng cách khai thác các lỗ hổng an toàn thông tin và thực hiện các cuộc tấn công mưu mô, nhóm đã chứng minh khả năng xâm nhập và gây nguy hiểm lên hệ thống mục tiêu.

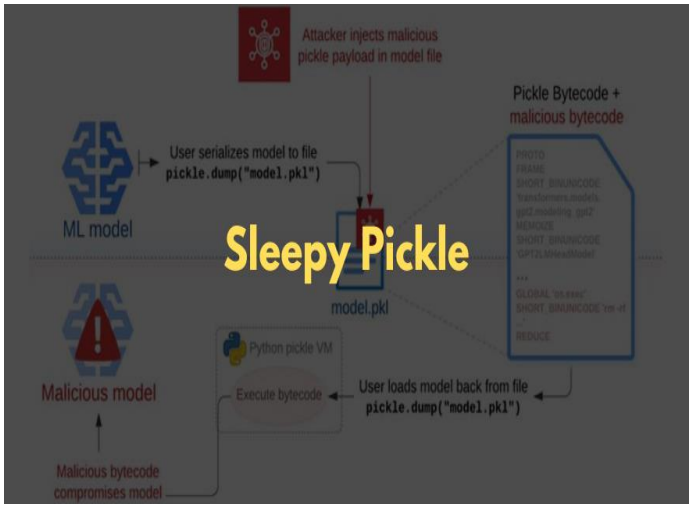
Một số IoC ghi nhận được:

hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF_update.hta	hxxp://mega.vlvlvlvl[.]site/HP.exe
hxxp://mega.vlvlvlvl[.]site/HPCustPartUI.dll	hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF.ps1
hxxp://payment.tripadviso[.]online/tempdata.dat	hxxp://vibm[.]vn/init.txt
hxxp://megacybernews[.]com/newrun.ps1	hxxp://megacybernews[.]com/getdata.ps1
hxxp://megacybernews[.]com/stage2.2.ps1	hxxp://megacybernews[.]com/checkin.php
hxxp://megacybernews[.]com/book.dll	hxxp://megacybernews[.]com/unikey.exe
hxxp://megacybernews[.]com/wwlib.dll	mega.vlvlvlvl[.]site
payment.tripadviso[.]online	vibm[.]vn
megacybernews[.]com	0

Nguồn: https://thecyberexpress.com/mustang-panda-target-vietnamese-firms/

Tin tức An toàn thông tin

"Cảnh báo: Sleepy Pickle - Mối đe dọa mới đối với các mô hình Machine Learning"



Gần đây, định dạng Pickle đang gây lo ngại về an toàn thông tin với phát hiện về kỹ thuật tấn công mới "Sleepy Pickle". Pickle thường được dùng để tuần tự hóa và phân phối mô hình học máy (ML), trở thành mục tiêu hấp dẫn cho các cuộc tấn công vì có thể bị lợi dụng để thực thi mã tùy ý khi giải tuần tự hóa. Các chuyên gia khuyến nghị người dùng chỉ nên tải mô hình từ nguồn tin cậy, sử dụng các mô hình có chữ ký số hoặc chuyển đổi từ các định dạng an toàn như Jax với cơ chế from_tf=True.

"Sleepy Pickle" là một kỹ thuật tấn công đặc biệt nhắm vào mô hình học máy bằng cách chèn payload độc hại vào file Pickle. Quá trình này thường được thực hiện thông qua các công cụ mã nguồn mở như Fickling. Sau đó, file Pickle độc hại này được phát tán đến nạn nhân thông qua nhiều phương pháp khác nhau, bao gồm:

- Adversary-in-the-Middle (AitM): Đối tượng tấn công đứng giữa quá trình truyền dữ liệu để chỉnh sửa hoặc chèn payload vào.
- Phishing: Dụ dỗ người dùng mở file Pickle độc hại qua email hoặc tin nhắn giả mạo.
- Xâm nhập chuỗi cung ứng: Chèn mã độc vào các file hợp lệ trong quá trình phân phối.
- Khai thác lỗ hổng hệ thống: Sử dụng các lỗ hổng bảo mật để tải file Pickle độc hại lên hệ thống mục tiêu.

Trong các kịch bản tấn công giả định, kỹ thuật "Sleepy Pickle" có thể dẫn đến những hậu quả nghiêm trọng. Ví dụ, nó có thể tạo ra những kết quả đầu ra độc hại hoặc thông tin sai lệch, như khuyên người dùng uống thuốc tẩy để chữa bệnh cúm, gây nguy hiểm đến tính mạng. Ngoài ra, kỹ thuật này cũng có thể được sử dụng để đánh cắp dữ liệu người dùng khi các điều kiện nhất định được đáp ứng, hoặc tấn công gián tiếp thông qua việc tạo ra các bản tóm tắt tin tức giả mạo có chứa liên kết dẫn đến các trang lừa đảo.

Nguồn: https://thehackernews.com/2024/06/new-attack-technique-sleepy-pickle.html

Tin tức An toàn thông tin

"Cảnh báo: Sleepy Pickle - Mối đe dọa mới đối với các mô hình Machine Learning"

"Sleepy Pickle" đặc biệt nguy hiểm vì nó cho phép kẻ tấn công duy trì quyền truy cập ẩn vào hệ thống ML. Mô hình bị lây nhiễm trong quá trình file Pickle được nạp vào Python, khiến kỹ thuật này hiệu quả hơn so với việc trực tiếp tải lên mô hình độc hại lên các nền tảng như Hugging Face. Điều này cho phép kẻ tấn công thay đổi hoạt động của mô hình hoặc kết quả tạo ra một cách linh hoạt mà không cần phải thuyết phục người dùng tải xuống và thực thi mô hình độc hại.

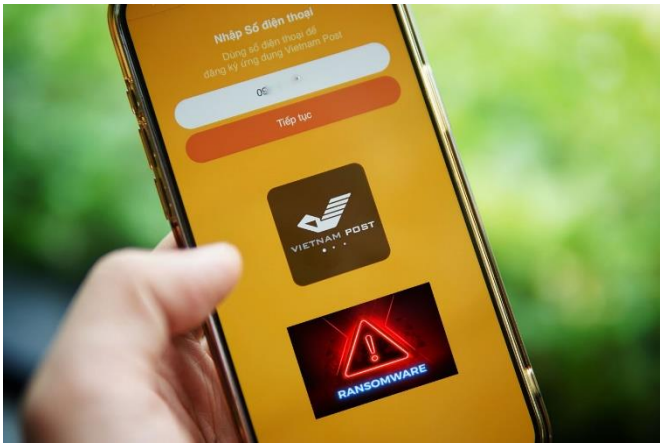
Ngoài "Sleepy Pickle", còn có một biến thể khác được gọi là "Sticky Pickle". Biến thể này thậm chí còn tinh vi hơn khi nó tích hợp một cơ chế tự sao chép, giúp duy trì sự hiện diện của payload độc hại trong các phiên bản mới của mô hình bị xâm nhập. Sticky Pickle sử dụng kỹ thuật làm mờ mã để tránh bị phát hiện bởi các công cụ quét file Pickle. Nhờ đó, ngay cả khi người dùng chỉnh sửa mô hình bị xâm nhập và phân phối lại nó qua một file Pickle mới, mã độc vẫn có thể tồn tại và tiếp tục tấn công.

Để phòng chống các cuộc tấn công như "Sleepy Pickle" và các cuộc tấn công chuỗi cung ứng khác, các chuyên gia khuyến nghị tránh sử dụng file Pickle để phân phối mô hình đã tuần tự hóa. Thay vào đó, chỉ nên sử dụng các mô hình từ các tổ chức đáng tin cậy và dựa vào các định dạng tệp an toàn hơn như SafeTensors. Việc tuân theo các khuyến nghị này sẽ giúp giảm thiểu rủi ro và bảo vệ hệ thống học máy khỏi các mối đe dọa tiềm ẩn.

Nguồn: https://thehackernews.com/2024/06/new-attack-technique-sleepy-pickle.html

Tin tức An toàn thông tin

"Thông tin: Hệ thống công nghệ thông tin của Bưu điện Việt Nam đã hoạt động trở lại"



Sau 3 ngày kể từ khi bị tin tặc tấn công mã hóa dữ liệu, hệ thống công nghệ thông tin phục vụ khách hàng và hoạt động quản lý vận hành của Bưu điện Việt Nam đã phục hồi

Theo thông báo của Tổng công ty Bưu điện Việt Nam (Vietnam Post), đến thời điểm 22h00 ngày 7/6/2024, hệ thống công nghệ thông tin phục vụ khách hàng và hoạt động quản lý vận hành của Bưu điện Việt Nam đã được phục hồi. Mọi hoạt động liên quan đến các dịch vụ đã cơ bản hoạt động bình thường và chưa ghi nhận bất cứ dấu hiệu thiệt hại về tài chính nào.

Hiện ứng dụng My Vietnam Post Plus vẫn đang được đồng bộ. Bưu điện Việt Nam cho biết sẽ có thông báo đến khách hàng trong thời gian sớm nhất.

Trước đó, vào 03h10 ngày 4/6/2024, hệ thống công nghệ thông tin của Tổng công ty Bưu điện Việt Nam đã bị tin tặc tấn công mã hóa dữ liệu (ransomware). Ngay khi phát hiện sự cố, Bưu điện Việt Nam đã nhanh chóng kích hoạt kịch bản hành động, bám sát theo hướng dẫn của Cục An toàn thông tin (Bộ Thông tin và Truyền thông), tập trung toàn lực để xử lý sự cố trong thời gian sớm nhất, đảm bảo tối đa quyền lợi khách hàng, giảm thiểu việc gián đoạn trong cung cấp dịch vụ.

Với sự hỗ trợ kịp thời và tích cực của Cục An toàn thông tin (Bộ Thông tin và Truyền thông), Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an, sự phối hợp chặt chẽ, hỗ trợ kịp thời của các đơn vị chuyên trách ATTT, cùng sự nỗ lực của đội ngũ cán bộ kỹ thuật, kỹ sư công nghệ, Bưu điện Việt Nam đã cô lập sự cố, bảo vệ dữ liệu, từng bước phục dựng hệ thống song song với việc điều tra, phân tích chuyên sâu nguyên nhân.

Đại diện Bưu điện Việt Nam cho biết, sự cố gây ảnh hưởng trực tiếp đến việc thực hiện các hoạt động liên quan đến dịch vụ bưu chính chuyển phát. Trong khi đó, các dịch vụ tài chính bưu chính, hành chính công và phân phối hàng hóa vẫn hoạt động bình thường.

Nguồn: https://vtv.vn/cong-nghe/he-thong-cong-nghe-thong-tin-cua-buu-dien-viet-nam-da-hoat-dong-tro-lai-20240609080055218.htm

Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất **690** lỗ hổng, trong đó có 127 lỗ hổng mức Cao, 311 lỗ hổng mức Trung bình, 14 lỗ hổng mức Thấp và 238 lỗ hổng chưa đánh giá. Trong đó có ít nhất 133 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của Telerik, ngôn ngữ lập trình PHP và Oracle, cụ thể là như sau:

- **CVE-2024-4358 (Điểm CVSS: 9.8 – Nghiêm trọng):** Là lỗ hổng bỏ qua bước xác thực tồn tại trên Progress Telerik Report Server phiên bản cũ hơn 2024 Q1 (10.0.24.305) trên IIS, cho phép đối tượng tấn công có thể truy cập và thực hiện các hành vi trái phép trên chức năng hạn chế của máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-4577 (Điểm CVSS: 9.8 – Nghiêm trọng):** Là lỗ hổng tồn tại trong ngôn ngữ lập trình PHP trên Apache và PHP-CGI của Windows. Lỗ hổng xảy ra do Windows sử dụng hành vi "Best-Fit" để thay thế kí tự trong command line cung cấp tới hàm Win32 API. Đối tượng tấn công có thể khai thác lỗ hổng để truyền các tùy chỉnh độc hại tới binary PHP qua đó biết được mã nguồn, thực thi đoạn mã PHP tùy ý trên máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thai thác trong thực tế.
- **CVE-2017-3506 (Điểm CVSS: 7.4 – Cao):** Lỗ hổng tồn tại trên thành phần Oracle WebLogic Server của Oracle Fusion Middleware cho phép đối tượng tấn công với khả năng truy cập vào hệ thống mạng của máy chủ qua giao thức HTTP, có thể truy cập và thực hiện các hành vi trái phép tới dữ liệu máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-4358	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Progress Telerik Report Server. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4358
2	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ngôn ngữ lập trình PHP. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4577
3	CVE-2017-3506	- Điểm CVSS: 7.4 (Cao) - Ảnh hưởng: Oracle Weblogic Server. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2017-3506
4	CVE-2024-26229	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows CSC - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-26229
5	CVE-2024-29849	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Veeam Backup Enterprise Manager - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-29849

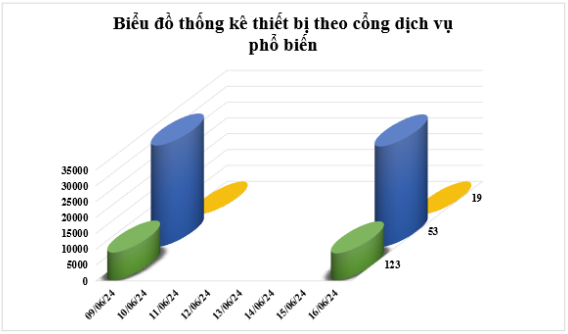
TOP 10 lỗ hổng đáng chú ý trong tuần

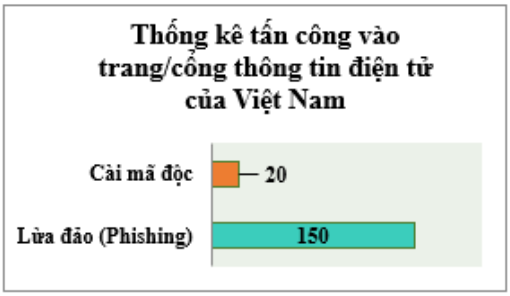
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-30078	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows CSC - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-30078
7	CVE-2024-3008	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Tenda - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3008
8	CVE-2024-26169	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-26169
9	CVE-2024-30080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-30080
10	CVE-2024-3700	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Estomed Simple Care - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3700

Thống kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **40.304** (giảm so với tuần trước **40.819**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.



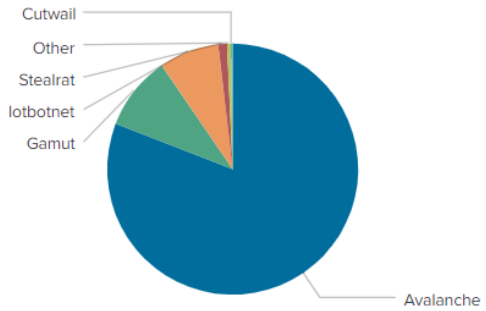


Tấn công Web

Trong tuần, có **170** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 150 trường hợp tấn công lừa đảo (Phishing), 20 trường hợp tấn công cài cắm mã độc.

Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.



Địa chỉ được sử dụng trong các mạng botnet

differentia.ru	xjpakmdcfuqe.in
disorderstatus.ru	dkmjxh.info
atomictrivia.ru	andall.servicesql.info
amnsreiuojy.ru	restless.su
xjpakmdcfuqe.biz	griefcube.cc
restlesz.su	tokyueiklbphqgupc.org
hzmksreiuojy.ru	rgbppxtvieoytnoej.org
ecishh.info	mcnodes.zapto.org
xjpakmdcfuqe.com	focusdate.com
xjpakmdcfuqe.ru	fefqkn.org

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **814** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) qua hệ thống tại địa chỉ https://canhbao.khonggianmang.vn. Qua kiểm tra, phân tích có nhiều trường hợp lừa đảo giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://shop[.]global-selling[.]top	Website giả mạo sàn TMĐT Amazon
2	https://thisinhthanhlich2024[.]com	Website giả mạo Facebook
3	https://duyetdonlazada[.]com	Website giả mạo sàn TMĐT Lazada
4	https://da8975[.]com	Website giả mạo sàn TMĐT Lazada
5	moneytracking137[.]com	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
6	cskhcanhanhd[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
7	https://mbdk99[.]com	Website giả mạo Ngân hàng TMCP Quân đội
8	https://www[.]dangnhaphoso[.]com	Website giả mạo Ngân hàng TMCP Quân đội
9	https://nang-cap-ocare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	vib-nangcap[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	main-card-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	www[.]vpbank[.]chamsockhachhang-uudaithecanhan-tructuyen[.]online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
13	https://www[.]tinchapshinhan[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
14	https://sendotv[.]com	Website giả mạo sàn TMĐT Sendo
15	https://sp1663p[.]com	Website giả mạo sàn TMĐT Shopee
16	https://www[.]vn999mall[.]vip	Website giả mạo sàn TMĐT Shopee
17	https://www[.]thanhtrapcrt[.]online	Website giả mạo Thanh tra Chính phủ
18	https://tdkt00[.]com	Website giả mạo sàn TMĐT Tiki
19	https://zla653[.]top	Website giả mạo sàn TMĐT Tiki
20	Giaodichquoctes[.]com	Website giả mạo Western Union

NCSC VN
National Cyber Security Center

Khuyến nghị đối với các cơ quan, đơn vị

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin tức an toàn thông tin,** Quý đơn vị cần thường xuyên cập nhật thông tin (như các chiến dịch tấn công của các nhóm APT, thông tin IoC kèm theo từng chiến dịch, điểm yếu lỗ hổng đang bị lợi dụng để khai thác,…), rà soát trên các hệ thống thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần Lỗ hổng bảo mật, Quý đơn vị cần lưu ý theo dõi và cập nhật bản vá cho các lỗ hổng liên quan đến sản phẩm đang sử dụng. Ngoài ra, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

3. Đối với các nguy cơ về tấn công từ chối dịch vụ, tấn công web trong phần **Thống kê nguy cơ, các cuộc tấn công tại Việt Nam**, Quý đơn vị cần rà soát, hạn chế tối đa việc mở các cổng dịch vụ có thể bị lợi dụng để thực hiện tấn công từ chối dịch vụ; thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và xử lý nguy cơ tấn công. Bên cạnh đó, đối với các IP/tên miền được đề cập trong mục **Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam**, Quý đơn vị cần kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại mà Cục ATTT đã chia sẻ.

***

4. Đối với các website giả mạo thống kê tại mục **Tấn công lừa đảo người dùng Việt Nam**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

024.3209.1616
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội