NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 50 (09/12/2024 – 15/12/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Ghi nhận chiến dịch tấn công với mục tiêu gián điệp không gian mạng nhằm vào các tổ chức tại Đông Nam Á.

- **Cảnh báo:** Ivanti đưa ra cảnh báo về lỗ hổng an toàn thông tin mức nghiêm trọng trên CSA cho phép đối tượng tấn công bỏ qua biện pháp xác thực.

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: 6.172** 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: Ghi nhận chiến dịch tấn công với mục tiêu gián điệp không gian mạng nhằm vào các tổ chức tại Đông Nam Á"

Gần đây, các chuyên gia bảo mật đã ghi nhận một chiến dịch tấn công được tình nghi là thực hiện bởi nhóm tấn công APT có liên kết với Trung Quốc, nhằm vào các tổ chức tại Đông Nam Á kể từ tháng 10/2023.

Cụ thể, chiến dịch tấn công nhằm vào các tổ chức thuộc nhiều lĩnh vực khác nhau của chính phủ tại hai quốc gia Đông Nam Á, một tổ chức quản lý không lưu, một công ty viễn thông và một trang truyền thông.

Chiến dịch tấn công này sử dụng bộ công cụ trước đó được xác định thuộc sở hữu của các nhóm APT Trung Quốc, với đặc điểm là mã nguồn mở và sử dụng kỹ thuật living-off-the-land. Bộ công cụ gồm có: các chương trình proxy đảo nghịch như Rakshasa và Stowaway, cũng như các công cụ có chức năng rà quét thiết bị, định danh, keylogger và đánh cắp mật khẩu.

Ngoài ra, nhóm APT này còn triển khai mã độc PlugX, một trojan truy cập từ xa phổ biến với các nhóm tấn công Trung Quốc.

Các chuyên gia bảo mật cũng ghi nhận nhóm đối tượng cài đặt các file DLL có chức năng làm bộ lọc bắt dữ liệu trên chức năng xác thực, cho phép đối tượng thu thập thông tin xác thực của người dùng. Trong một trường hợp tấn công diễn ra từ tháng 06/2024 đến tháng 08/2024, nhóm này đã thực hiện hành vi do thám và trích xuất mật khẩu, cùng với cài đặt keylogger, thực thi các payload DLL với chức năng thu thập thông tin xác thực của người dùng.

Việc nhóm tấn công này duy trì truy cập một cách bí mật tới các hệ thống mạng bị xâm nhập trong một khoảng thời gian dài đã cho phép nhóm thu thập thông tin và sơ đồ hóa hệ thống mạng của tổ chức. Các thông tin này được nén lại và bảo vệ mật khẩu sử dụng WinRAR rồi tải lên các nền tảng lưu trữ cloud như File.io.

Nguồn: https://thehackernews.com/2024/12/researchers-uncover-espionage-tactics.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Ghi nhận chiến dịch tấn công với mục tiêu gián điệp không gian mạng nhằm vào các tổ chức tại Đông Nam Á"

Các chuyên gia bảo mật cũng cho biết, việc các nhóm tấn công tại Trung Quốc cùng dùng chung bộ công cụ, kỹ thuật tấn công khiến việc xác định chính xác nhóm tấn công trở nên khó khăn hơn. Tình hình chính trị căng thẳng tại Đông Nam Á, cụ thể là khu vực Thái Bình Dương, được nêu bật bởi các chiến dịch tấn công thực hiện bởi các nhóm như Unfading Sea Haze, Mustang Panda, CeranaKeeper và chiến dịch Crimson Palace trong thời gian gần đây nhằm vào khu vực này.

Thông tin về chiến dịch tấn công này được công bố trong bối cảnh một cơ quan bảo mật khác công bố thông tin về nhóm gián điệp không gian mạng của Trung Quốc nhằm vào nhà cung cấp dịch vụ IT tại châu Âu trong chiến dịch Digital Eye.

Một số IoC được ghi nhận:

38.60.146[.]78:443	118.107.219[.]66:443
45.123.188[.]180	198.244.237[.]131

Nguồn: https://thehackernews.com/2024/12/researchers-uncover-espionage-tactics.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Ivanti đưa ra cảnh báo về lỗ hổng an toàn thông tin mức nghiêm trọng trên CSA cho phép đối tượng tấn công bỏ qua biện pháp xác thực"

Gần đây, hãng Ivanti đã đưa ra cảnh báo về lỗ hổng an toàn thông tin mức nghiêm trọng tồn tại trên giải pháp Cloud Services Appliance (CSA) cho phép đối tượng tấn công bỏ qua biện pháp xác thực khi khai thác thành công.

Lỗ hổng có mã định danh CVE-2024-11369 cho phép đối tượng tấn công đạt được quyền quản trị trên giải pháp Ivanti CSA phiên bản 5.0.2 hoặc cũ hơn mà không cần tới sự tương tác của người dùng. Hãng cũng khuyến nghị người dùng cập nhật bản vá sớm nhất có thể để tránh bị ảnh hưởng bởi các cuộc tấn công.

Tuy nhiên, được biết hiện chưa có người dùng nào được ghi nhận là bị ảnh hưởng bởi tấn công sử dụng lỗ hổng này, ngoài ra lỗ hổng cũng chưa có mã khai thác công khai.

Ngoài lỗ hổng này, Ivanti cũng đã vá một số lỗ hổng khác ở các mức độ Trung bình, Cao và Nghiêm trọng trên Desktop and Server Management (DSM), Connect Secure and Policy Secure, Sentry và các sản phẩm thuộc Patch SDK.

Lỗ hổng CVE-2024-11369 là lỗ hổng thứ 6 tồn tại trên CSA được vá trong những tháng gần đây của hãng Ivanti. Đặc biệt, hai lỗ hổng CVE-2024-8190 và CVE-2024-8963 trước đó đã bị khai thác trong chiến dịch tấn công thực tế và ba lỗ hổng CVE-2024-9379, CVE-2024-9380, CVE-2024-9381 được khai thác trong chuỗi tấn công với lỗ hổng CVE-2024-8963 để khai thác lỗi SQL Injection dẫn tới việc bỏ qua biện pháp bảo mật và thực thi mã từ xa thông qua Command Injection.

Luồng lỗ hổng bị khai thác trong thực tế được phát hiện khi Ivanti cho biết họ đã tăng cường khả năng kiểm tra và quét nội bộ, đồng thời đang cải thiện quy trình tiết lộ có trách nhiệm để vá các lỗi bảo mật nhanh hơn. Một số lỗ hổng khác đã bị khai thác dưới dạng zero-day trong các cuộc tấn công rộng rãi vào đầu năm nay trong các chiến dịch nhắm mục tiêu vào các thiết bị Ivanti VPN và các cổng ICS, IPS và ZTA.

Nguồn: https://www.bleepingcomputer.com/news/security/ivanti-warns-of-maximum-severity-csa-auth-bypass-vulnerability/

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 **1.282** lỗ hổng, trong đó có 191 lỗ hổng mức Cao, 303 lỗ hổng mức Trung bình, 10 lỗ hổng mức Thấp và 778 lỗ hổng chưa đánh giá. Trong đó có ít nhất 265 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 ProjectSend, MiTel, Cleo Harmony, VLTrader và Lexicom, cụ thể là như sau:

- **CVE-2024-11680 (Điểm CVSS: Chưa xác định):** Lỗ hổng tồn tại trên ProjectSend tồn tại do thiếu sót trong khâu xác thực, đối tượng tấn công khai thác thành công lỗ hổng có thể truy cập và thực hiện các hành vi trái phép như tạo tài khoản tùy ý, tải lên các webshell độc hại và nhúng JavaScript độc hại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-41713 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên thành phần NuPoint Unified Messaging (NPM) của Mitel MiCollab cho phép đối tượng tấn công khai thác thực hiện tấn công Path Travelsal, từ đó dẫn tới việc truy cập và thực hiện các hành vi trái phép như xem, làm hỏng hoặc xóa cấu hình hệ thống, dữ liệu người dùng. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-50263 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Cleo Harmony, VLTrader và LexiCom cho phép đối tượng tấn công chèn đoạn mã JavaScript độc hại thông qua thức năng tải lên, tải xuống file từ đó dẫn tới thực thi mã từ xa. 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-2024-41713	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Mitel MiCollab - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Lỗ hổng chưa 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-2024-41713
2	CVE-2024-11680	- Điểm CVSS: Chưa xác định - Ảnh hưởng: ProjectSends - 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-2024-11680
3	CVE-2024-50623	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Cleo Harmony, VLTrader và LexiCom - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - 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-2024-50623
4	CVE-2024-49116	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa 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-2024-49116
5	CVE-2024-49138	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Lỗ hổng chưa 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-2024-49138

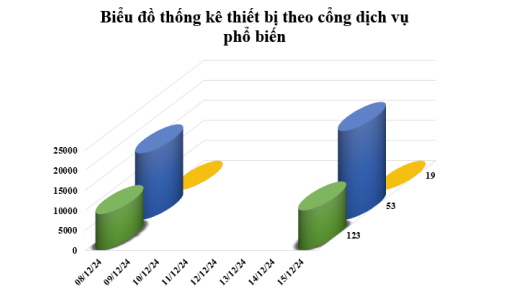
TOP 10 lỗ hổng đáng chú ý trong tuần

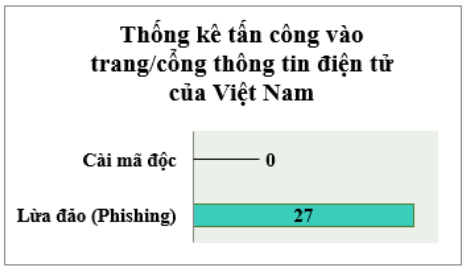
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-49112	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-49112
7	CVE-2024-54143	- Điểm CVSS: 9.3 (Nghiêm trọng) - Ảnh hưởng: OpenWrt - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Lỗ hổng chưa 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-2024-54143
8	CVE-2024-53677	- Điểm CVSS: 9.5 (Nghiêm trọng) - Ảnh hưởng: Apache Struts - 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-2024-53677
9	CVE-2024-49106	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa 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-2024-49106
10	CVE-2024-49108	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa 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-2024-49108

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 **32.060** (tăng so với tuần trước **25.615**) 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.



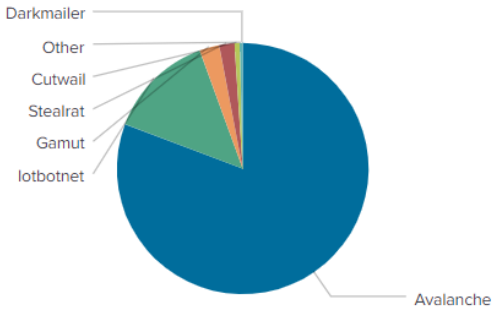


Tấn công Web

Trong tuần, có **27** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 27 trường hợp tấn công lừa đảo (Phishing), 0 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

disorderstatus.ru	morphed.ru
differentia.ru	gjogvvpsf.biz
atomictrivia.ru	ygiudewsqhct.in
a.asense.in	xjpakmdcfuqe.biz
sdk.asense.in	hzmksreiuojy.ru
statis.multispacesext.net	yunalwv.biz
ipjfhqda.info	hzmksreiuojy.in
amnsreiuojy.ru	a.deltaheavy.ru
thesecond.in	restlesz.su
cp.14b3x6oa.ru	gytujflc.biz

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **6.172** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **284** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **5.888** trường hợp phản ánh cuộc gọi, tin nhắn lừa đảo thông qua tổng đài 156/5656

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

STT	Website lừa đảo	Ghi chú
1	https://sellings-global[.]com/shop	Website giả mạo sàn TMĐT Amazon
2	vietchinhphu[.]com	Website giả mạo Cổng Dịch vụ công Quốc gia
3	https://chat[.]dichvutonghop[.]vip/mobile/index?code=5dNnwAlZmXa8ELYdy3FnUESBYQgLpcZ5jKi4MYA3XOG1NLxUpNmNLWcmz12qHQoQlj2s4iXw%2FzjgvtmomDR0VshLNZtBAxBLxRoBsOnRh8%2FS7vKKZuG9lF1RoudmuJT4X%2Fc	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	aeonmaills[.]shop	Công ty TNHH Aeon Việt Nam
5	https://www[.]ebayglobal[.]shop/home	Website giả mạo sàn TMĐT Ebay
6	https://giaohangnhanh88[.]com/	Website giả mạo Giao hàng nhanh
7	https://thuongmdientu[.]shop/index/index/home[.]html	Website giả mạo sàn TMĐT Lazada
8	https://da5651[.]com	Website giả mạo sàn TMĐT Lazada
9	xjp[.]morganfutureszy[.]com	Website giả mạo Ngân hàng JP Morgan Chase Bank Mỹ tại Việt Nam
10	https://cskh-techcombank[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
11	hdbank[.]khuyenmaikhachhang-triankhachhang-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
12	https://mbtaichinh-tienloi[.]com/	Website giả mạo Ngân hàng TMCP Quân đội
13	https://tc-shbfinance[.]com/	Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội
14	vpbank[.]hotrotructuyen-chamsockhachhang-hotro247-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
15	mail[.]vpbank[.]hotrotructuyen-chamsockhachhang-hotro247-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
16	https://shinhan[.]hotrokhachhang-hotrotructuyen-uudaidacbiet-thang12[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
17	www[.]sp66699[.]com	Website giả mạo sàn TMĐT Shopee
18	https://sp6708p[.]com	Website giả mạo sàn TMĐT Shopee
19	https://sp5583p[.]com	Website giả mạo sàn TMĐT Shopee
20	chinhphuvn[.]cc	Website giả mạo Văn phòng Chính phủ

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