NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 44 (28/10/2024 – 03/11/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Evasive Panda sử dụng bộ công cụ CloudScout để đánh cắp cookie phiên đăng nhập từ các dịch vụ đám mây.

- **Cảnh báo:** Lỗ hổng RCE trên Microsoft Sharepoint bị khai thác để xâm nhập vào hệ thống mạng của doanh nghiệp.

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: 2784** 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 Evasive Panda sử dụng bộ công cụ CloudScout để đánh cắp cookie phiên đăng nhập từ các dịch vụ đám mây"

Gần đây, các tổ chức chính phủ và tôn giáo tại Đài Loan đã trở thành mục tiêu của nhóm APT Evasive Panda có nguồn gốc từ Trung Quốc. Trong chiến dịch tấn công này, Evasive Panda sử dụng bộ công cụ hậu khai thác có tên CloudScout để xâm nhập và thu thập dữ liệu.

Bộ công cụ này có khả năng thu thập dữ liệu từ nhiều dịch vụ đám mây khác nhau nhờ vào các cookie phiên web bị đánh cắp. Thông qua một plugin, CloudScout hoạt động đồng bộ với MgBot – bộ khung mã độc đặc trưng của nhóm Evasive Panda.

ESET phát hiện rằng mã độc dựa trên nền tảng .NET này đã xuất hiện từ khoảng tháng 05/2022 đến tháng 02/2023, với tổng cộng 10 module viết bằng C#, trong đó có ba module chuyên thu thập dữ liệu từ Google Drive, Gmail và Outlook.

Evasive Panda, còn được biết đến với tên gọi Bronze Highland, Daggerfly, và StormBamboo, là một nhóm gián điệp mạng chuyên tấn công vào các tổ chức tại Đài Loan và Hồng Kông. Nhóm này cũng nổi tiếng với các cuộc tấn công watering hole và chuỗi cung ứng, đặc biệt nhắm vào cộng đồng người Tây Tạng.

Điểm nổi bật của nhóm APT Evasive Panda là khả năng triển khai nhiều phương thức tấn công, bao gồm khai thác các lỗ hổng bảo mật mới công bố và tấn công chuỗi cung ứng bằng DNS poisoning, nhằm xâm nhập vào mạng lưới nạn nhân và triển khai MgBot và Nightdoor.

Phân tích cho thấy, các module CloudScout được thiết kế để chiếm dụng các phiên đã được xác thực trên trình duyệt web bằng cách đánh cắp cookie và sử dụng chúng để truy cập trái phép vào Google Drive, Gmail và Outlook. Các module này được triển khai qua một plugin của MgBot viết bằng C++.

CloudScout được xây dựng dựa trên gói CommonUtilities, cung cấp các thư viện cần thiết ở cấp độ thấp cho các module hoạt động, bao gồm:

Nguồn: https://thehackernews.com/2024/10/chinese-hackers-use-cloudscout-toolset.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Evasive Panda sử dụng bộ công cụ CloudScout để đánh cắp cookie phiên đăng nhập từ các dịch vụ đám mây"

- HTTPAccess – hàm xử lý kết nối giao thức HTTP;
- ManagedCookie – hàm quản lý cookie cho các yêu cầu web giữa CloudScout và dịch vụ mục tiêu;
- Logger;
- SimpleJSON.

Dữ liệu được thu thập từ ba module – bao gồm danh sách thư mục thư, email (kèm theo tệp đính kèm), và các tệp có định dạng nhất định (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf và .txt) – sẽ được nén thành file ZIP trước khi trích xuất thông qua MgBot hoặc Nightdoor.

Những cơ chế bảo mật mới do Google phát hành, như Device Bound Session Credentials (DBSC) và App-Bound Encryption, dự kiến sẽ làm cho các mã độc dựa trên cookie trở nên lỗi thời.

Thông tin về nhóm tấn công Evasive Panda và bộ công cụ CloudScout được công bố trong bối cảnh chính phủ Canada cáo buộc một nhóm tấn công có liên quan đến Trung Quốc đã tiến hành các hoạt động do thám kéo dài nhiều tháng trên nhiều lĩnh vực tại quốc gia này.

Một số IoC được ghi nhận:

103.96.128[.]44	C70C3750AC6B9D7B033ADDEF838EF1CC28C262F3	812124B84C5EA455F7147D94EC38D24BDF159F84
AD6C84859D413D627AC589AEDF9891707E179D6C	3DD958CA6EB7E8F0A0612D295453A3A10C08F5FE	547BD65EEE05D744E075C5E12FB973A74D42438F
348730018E0A5554F0F05E47BBA43DC0F55795AC	9B6A473820A72111C1A38735992B55C413D941EE	621E2B50A979D77BA3F271FAB94326CCCBC009B4
C058F9FE91293040C8B0908D3DAFC80F89D2E38B	4A5BCDAAC0BC315EDD00BB1FCCD1322737BCBEEB	67028AEB095189FDF18B2D7B775B62366EF224A9
B3556D1052BF5432D39A6068CCF00D8C318AF146	84F6B9F13CDCD8D9D15D5820536BC878CD89B3C8	93C1C8AD2AF64D0E4C132F067D369ECBEBAE00B7
8EAA213AE4D482938C5A7EC523C83D2C2E1E8C0E	A1CA41FDB61F03659168050DE3E208F0940F37D8	0

Nguồn: https://thehackernews.com/2024/10/chinese-hackers-use-cloudscout-toolset.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng RCE trên Microsoft Sharepoint bị khai thác để xâm nhập vào hệ thống mạng của doanh nghiệp"

Gần đây, các chuyên gia bảo mật đã ghi nhận lỗ hổng RCE (thực thi mã từ xa) có mã CVE-2024-38094 bị khai thác trong thực tế nhằm đạt quyền truy cập tới hệ thống mạng doanh nghiệp.

Lỗ hổng CVE-2024-38094 (Điểm CVSS: 7.2) là một lỗ hổng RCE ảnh hưởng đến Microsoft SharePoint, nền tảng web phổ biến được sử dụng làm hệ thống mạng nội bộ, quản lý tài liệu và công cụ hợp tác có khả năng tích hợp với Microsoft 365. Microsoft đã phát hành bản vá vào ngày 9/7/2024 trong đợt cập nhật Patch Tuesday tháng 7. Lỗ hổng này cũng đã được CISA thêm vào danh sách KEV vào tuần trước, nhưng chi tiết về cách khai thác chưa được tiết lộ.

Theo phân tích, đã phát hiện đối tượng tấn công đã lợi dụng lỗ hổng này để truy cập trái phép vào máy chủ SharePoint và cài đặt webshell, sử dụng mã khai thác PoC đã được công khai.

Sau khi truy cập được vào hệ thống, đối tượng tấn công tiến hành leo thang đặc quyền bằng cách chiếm quyền của một tài khoản dịch vụ Microsoft Exchange có quyền quản trị domain, từ đó gia tăng khả năng kiểm soát.

Tiếp đến, đối tượng cài đặt phần mềm diệt virus Huorong nhằm tạo xung đột, vô hiệu hóa các giải pháp bảo mật hiện có và giúp họ cài đặt Impacket để di chuyển ngang qua hệ thống. Với quyền kiểm soát, đối tượng sử dụng Mimikatz để thu thập thông tin xác thực, FRP để truy cập từ xa và thiết lập các tác vụ định kỳ để duy trì kết nối.

Trong bối cảnh lỗ hổng đang bị khai thác trong thực tế như trên, các quản trị viên hệ thống được khuyến nghị cập nhật SharePoint sớm nhất có thể để đảm bảo an toàn cho hệ thống.

Nguồn: https://www.bleepingcomputer.com/news/security/microsoft-sharepoint-rce-bug-exploited-to-breach-corporate-network/

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 **958** lỗ hổng, trong đó có 306 lỗ hổng mức Cao, 430 lỗ hổng mức Trung bình, 13 lỗ hổng mức Thấp và 209 lỗ hổng chưa đánh giá. Trong đó có ít nhất 153 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 FortiManager, Google Chrome và Labstack, cụ thể là như sau:

- **CVE-2024-47575 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên FortiManager cho phép đối tượng thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-4947 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Google Chrome là lỗ Type Confusion trên V8 cho phép đối tượng tấn công thực thi mã từ xa trong môi trường sandbox. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2022-40083 (Điểm CVSS: 9.6 – Nghiêm trọng):** Lỗ hổng tồn tại Labstack Echo là lỗi điều hướng mở cho phép đối tượng tấn công thực hiện SSRF lên hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: FortiManager - 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-2024-47575
2	CVE-2024-4947	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - 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-2024-4947
3	CVE-2022-40083	- Điểm CVSS: 9.6 (Nghiêm trọng) - Ảnh hưởng: Labstack Echo - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SSRF - 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-2022-40083
4	CVE-2024-40766	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: SonicWall SonicOS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - 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-2024-40766
5	CVE-2024-38812	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: VMware vCenter Server - 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-2024-38812

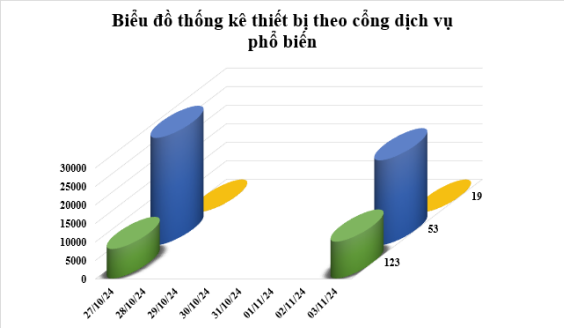
TOP 10 lỗ hổng đáng chú ý trong tuần

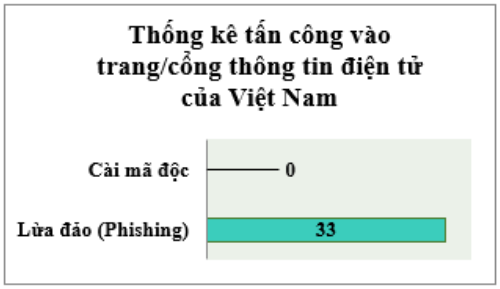
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-23113	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Fortinet FortiOS, FortiProxy, FortiPAM, và FortiSwitchManager - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-23113
7	CVE-2024-20481	- Điểm CVSS: 5.8 (Trung bình) - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - 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-2024-20481
8	CVE-2024-50550	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache - Mô tả: Lỗ hổng cho phép đối tượng 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-2024-50550
9	CVE-2024-10487	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - 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-2024-10487
10	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 thực thi mã từ xa, 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

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 **32.883** (giảm so với tuần trước **36.974**) 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.



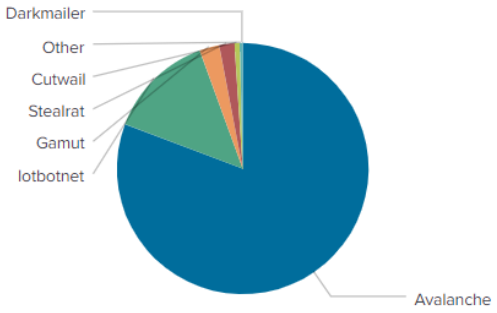


Tấn công Web

Trong tuần, có **33** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 33 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	ygiudewsqhct.in
atomictrivia.ru	hzmksreiuojy.ru
a.asense.in	xjpakmdcfuqe.biz
sdk.asense.in	hzmksreiuojy.in
statis.multispacesext.net	vptdjfz2w.ru
egksyqv.info	a.deltaheavy.ru
amnsreiuojy.ru	restlesz.su
thesecond.in	yunalwv.biz
gjogvvpsf.biz	atb-lit.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **2784** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **201** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **2583** 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	shop[.]shopamzselling[.]com	Website giả mạo sàn TMĐT Amazon
2	clash-flow-loan[.]com	Website giả mạo Bộ Công an
3	giaohangtietkiem-cskh[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	dienmayxanh-services[.]com	Website giả mạo Điện máy xanh
5	lazada[.]ac	Website giả mạo sàn TMĐT Lazada
6	lazada2024[.]online	Website giả mạo sàn TMĐT Lazada
7	vpbank[.]cskhtructuyen-uudaithang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
8	https://www[.]tb88789[.]com	Website giả mạo sàn TMĐT Shopee
9	https://www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
10	s[.]shopee[.]vn	Website giả mạo sàn TMĐT Shopee
11	sp5583p[.]com	Website giả mạo sàn TMĐT Shopee
12	www[.]evnnpcs[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
13	evn[.]brvgov[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
14	korshoptiktok[.]com	Website giả mạo Tik tok
15	tikione[.]vip	Website giả mạo sàn TMĐT Tiki
16	tikifreeship[.]xyz	Website giả mạo sàn TMĐT Tiki
17	www[.]tikifreeship[.]cc	Website giả mạo sàn TMĐT Tiki
18	topcvvn[.]com	Website giả mạo Top CV
19	vnairlines[.]net	Website giả mạo Vietnam Airlines
20	vneid[.]vieegovn[.]cc	Website giả mạo VNeID

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