NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 42 (14/10/2024 – 20/10/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT SideWinder tấn công nhằm vào vùng Trung Đông và Châu Phi trong chiến dịch tấn công đa giai đoạn.

- **Cảnh báo:** Lỗ hổng nghiêm trọng trên Kubernetes Image Builder khiến các Nodes trên giải pháp chịu rủi ro từ việc truy cập Root trái phép.

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: 190** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

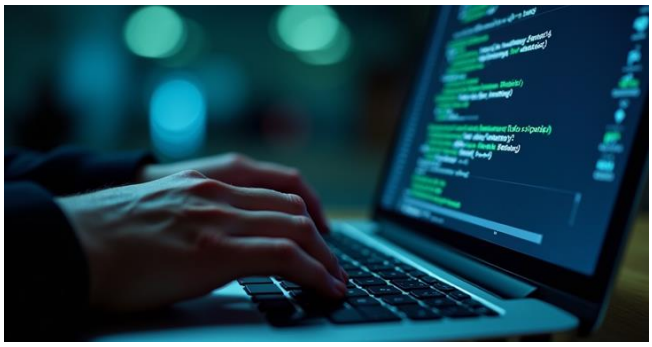
4. Tài liệu lưu trữ

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

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT SideWinder tấn công nhằm vào vùng Trung Đông và Châu Phi trong chiến dịch tấn công đa giai đoạn"



Các chuyên gia bảo mật đã phát hiện một nhóm APT có tên SideWinder có nguồn gốc từ Ấn Độ, nhóm này thực hiện hàng loạt cuộc tấn công nhắm vào các tổ chức và cơ sở hạ tầng quan trọng tại Trung Đông và châu Phi.

Nhóm APT SideWinder được biết đến với nhiều tên khác như APT-C-17, Baby Elephant, Hardcore Nationalist, Leafperforator, Rattlesnake, Razor Tiger, and T-APT-04. Các đối tượng bị tấn công chủ yếu thuộc các tổ chức chính phủ, quân đội, các công ty logistics, viễn thông, tài chính, các trường đại học, và các doanh nghiệp giao dịch dầu mỏ tại các quốc gia Bangladesh, Djibouti, Jordan, Malaysia, Maldives, Myanmar, Nepal, Pakistan, Ả Rập Saudi, Sri Lanka, Thổ Nhĩ Kỳ và Các Tiểu vương quốc Ả Rập Thống nhất (UAE). Ngoài ra, SideWinder còn nhắm đến các cơ quan ngoại giao tại Afghanistan, Pháp, Trung Quốc, Ấn Độ, Indonesia, và Ma-rốc.

Điểm nổi bật trong chiến dịch này là chiến thuật tấn công nhiều giai đoạn, với mục tiêu phát tán một loại mã độc mới có tên StealerBot, được tạo ra đặc biệt để thực hiện các hoạt động gián điệp phức tạp.

Chiến dịch tấn công bắt đầu bằng các email giả mạo (spear-phishing) chứa tệp đính kèm độc hại. Các tệp đính kèm này có thể là tệp nén ZIP chứa tệp shortcut Windows (LNK) hoặc tài liệu Microsoft Office. Khi nạn nhân mở tệp, chuỗi tấn công được kích hoạt, bắt đầu từ việc chạy các đoạn mã JavaScript và trình tải .NET, cuối cùng dẫn đến việc cài đặt mã độc StealerBot.

Tài liệu đính kèm trong email sử dụng kỹ thuật chèn mẫu từ xa để tải xuống một tệp RTF từ máy chủ do đối tượng tấn công kiểm soát. Tệp RTF này sẽ khai thác lỗ hổng CVE-2017-11882, cho phép thực thi mã JavaScript có nhiệm vụ kích hoạt thêm mã JavaScript khác từ trang web mofa-gov-sa.direct888[.]net. Trong trường hợp sử dụng tệp .LNK, nó sẽ sử dụng công cụ mshta.exe, một thành phần trên Windows được thiết kế để chạy các tệp Microsoft HTML Application (HTA), nhằm thực thi mã JavaScript độc hại từ máy chủ của đối tượng tấn công.

Nguồn: https://thehackernews.com/2024/10/sidewinder-apt-strikes-middle-east-and.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT SideWinder tấn công nhằm vào vùng Trung Đông và Châu Phi trong chiến dịch tấn công đa giai đoạn"

Mã độc JavaScript này được thiết kế để trích xuất một chuỗi nhúng, đã được mã hóa bằng Base64, và nó chính là thư viện .NET mang tên "App.dll". Thư viện này có nhiệm vụ thu thập thông tin hệ thống và đóng vai trò là bộ tải cho payload .NET từ máy chủ, được gọi là "ModuleInstaller.dll". Payload này cũng hoạt động như một bộ tải, nhưng nó còn có khả năng duy trì kết nối với hệ thống, thực thi module backdoor loader và tải về các thành phần cần thiết cho giai đoạn lây nhiễm tiếp theo. Cách thức hoạt động của nó sẽ phụ thuộc vào các giải pháp bảo mật endpoint đang được cài đặt trên hệ thống.

Mục tiêu cuối cùng của chiến dịch này là phát tán mã độc StealerBot thông qua module Backdoor loader. Mã độc này được lập trình bằng .NET và được mô tả là một "phần cài cắm nâng cao với tính năng mô-đun," nhằm thực hiện các hoạt động gián điệp thông qua việc tích hợp các plugin cho những hành vi sau:

- Cài đặt mã độc mới bằng bộ tải C++
- Chụp màn hình
- Ghi lại dữ liệu từ việc gõ phím
- Đánh cắp mật khẩu từ trình duyệt
- Chặn bắt thông tin xác thực RDP
- Đánh cắp tệp
- Khởi tạo reverse shell
- Giả mạo thông tin xác thực của Windows
- Leo thang đặc quyền truy cập trên hệ thống và vượt qua bảo mật của UAC.

Mã độc này bao gồm nhiều module được quản lý bởi thành phần chính gọi là "Orchestrator". Orchestrator có nhiệm vụ giao tiếp với máy chủ C&C để thực thi và quản lý các plugin. Orchestrator thường được tải lên thông qua module backdoor.

Ngoài ra, Kaspersky đã phát hiện hai thành phần "InstallerPayload" và "InstallerPayload_NET" tuy không nằm trong chuỗi tấn công chính nhưng có thể được sử dụng để cài đặt hoặc cập nhật StealerBot, hoặc lây nhiễm sang người dùng khác.

Nhóm APT SideWinder đang mở rộng phạm vi tấn công và sử dụng các công cụ phức tạp mới, trùng hợp với báo cáo từ Cyfirma về nhóm APT36 (Transparent Tribe) có nguồn gốc từ Pakistan. APT36 phát tán tệp Linux giả mạo dưới dạng PDF để tải xuống mã độc và duy trì kết nối lâu dài trên hệ thống mục tiêu. Nhóm này đã gia tăng nhắm vào các hệ thống Linux, đặc biệt là các hệ điều hành dựa trên Debian như BOSS OS và Maya OS, thường được sử dụng trong các cơ quan chính phủ Ấn Độ. Sự tương đồng trong hoạt động giữa hai nhóm cho thấy một xu hướng đáng lo ngại trong việc tấn công các mục tiêu quan trọng.

Nguồn: https://thehackernews.com/2024/10/sidewinder-apt-strikes-middle-east-and.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT SideWinder tấn công nhằm vào vùng Trung Đông và Châu Phi trong chiến dịch tấn công đa giai đoạn"

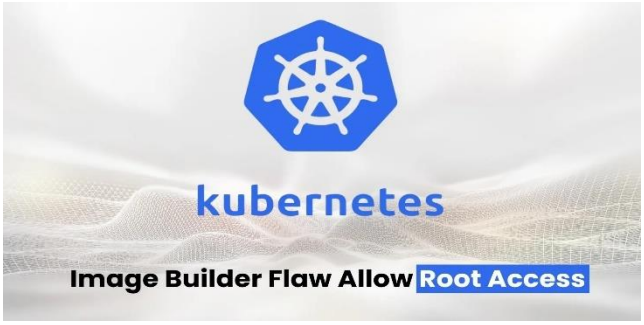
Một số IoC được ghi nhận:

126-com[.]live	163inc[.]com	afmat[.]tech	newoutlook[.]live
alit[.]live	aliyum[.]tech	aliyumm[.]tech	ntcpak[.]org
asyn[.]info	ausibedu[.]org	bol-south[.]org	numpy[.]info
cnsa-gov[.]org	colot[.]info	comptes[.]tech	office-drive[.]live
condet[.]org	conft[.]live	dafpak[.]org	paknavy-govpk[.]info
decoty[.]tech	defenec[.]net	defpak[.]org	pdfrdr-update[.]info
detru[.]info	dgps-govpk[.]co	dgps-govpk[.]com	pmd-office[.]org
dinfed[.]co	dirctt88[.]co	dirctt88[.]net	shipping-policy[.]info
direct888[.]net	direct88[.]co	directt888[.]com	tazze[.]co
donwload-file[.]com	donwloaded[.]com	donwloaded[.]net	tsinghua-edu[.]tech
dowmload[.]net	downld[.]net	download-file[.]net	ujsen[.]net
downloadabledocx[.]com	dynat[.]tech	dytt88[.]org	widge[.]info
e1ix[.]mov	e1x[.]tech	fia-gov[.]com	pafgovt[.]com
fia-gov[.]net	gov-govpk[.]info	govpk[.]info	paknavy-govpk[.]net
govpk[.]net	grouit[.]tech	gtrec[.]info	pmd-office[.]com
healththebest[.]com	jmicc[.]xyz	kernet[.]info	ptcl-net[.]com
kretic[.]info	lforvk[.]com	mfa-gov[.]info	sjfu-edu[.]co
mfa-gov[.]net	mfa-govt[.]net	mfacom[.]org	tex-ideas[.]info
mfagov[.]org	mfas[.]pro	mitlec[.]site	tumet[.]info
mod-gov-pk[.]live	mofa[.]email	mofagovs[.]org	update-govpk[.]co
moittpk[.]net	moittpk[.]org	mshealthcheck[.]live	paknavy-gov[.]org
nactagovpk[.]org	navy-mil[.]co	newmofa[.]com	pdfrdr-update[.]com
updtesession[.]online	nopler[.]live	ntcpak[.]live	pmd-office[.]live
tni-mil[.]com	ntcpk[.]info	ntcpk[.]net	scrabt[.]tech
u1x[.]co	numzy[.]net	nventic[.]info	support-update[.]info

Nguồn: https://thehackernews.com/2024/10/sidewinder-apt-strikes-middle-east-and.html

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng nghiêm trọng trên Kubernetes Image Builder khiến các Nodes trên giải pháp chịu rủi ro từ việc truy cập Root trái phép"



Các chuyên gia bảo mật đã ghi nhận lỗ hổng an toàn thông tin mức nghiêm trọng tồn tại trên Kubernetes Image Builder khi khai thác thành công sẽ cho phép đối tượng tấn công đạt được quyền truy cập root.

Lỗ hổng có mã CVE-2024-9486 (Điểm CVSS: 9.8) hiện đã được vá trong phiên bản 0.1.38. Cụ thể, lỗ hổng là lỗi thông tin xác thực mặc định được sử dụng trong quá trình xây dựng ảnh của máy ảo. Ngoài ra, các ảnh của máy ảo được dựng bởi Proxmox không vô hiệu hóa các thông tin xác thực này và các node sử dụng ảnh được tạo có thể bị truy cập sử dụng thông tin này vào thẳng quyền root.

Lỗ hổng chỉ gây ảnh hưởng tới các cụm Kubernetes có node sử dụng ảnh của máy ảo (VM) được tạo thông qua Image Builder do Proxmox cung cấp. Để tạm thời ngăn chặn lỗ hổng, người dùng được khuyến nghị nên tắt các tài khoản dựng ảnh trên các VM. Người dùng cũng nên xây lại các ảnh của máy ảo bằng phiên bản đã được vá của Image Builder rồi triển khai lại chúng trên máy ảo của mình.

Bản vá do Kubernetes phát hành đã thay đổi thông tin xác thực mặc định thành một chuỗi mật khẩu được tạo ngẫu nhiên trong quá xây dựng ảnh. Ngoài ra, tài khoản dùng trong quá trình cũng được vô hiệu hóa sau khi hoàn thành mục tiêu.

Kubernetes Image Builder phiên bản 0.1.38 cũng đã vá một lỗ hổng có liên quan với mã CVE-2024-9594 (Điểm CVSS: 6.3) về việc thông tin xác thực mặc định được sử dụng khi dựng ảnh sử dụng Nutanix, OVA, QEMU.

Thông tin về lỗ hổng được công bố trong lúc Microsoft phát hành bản vá phía server cho ba lỗ hổng nghiêm trọng trên Dataverse, Imagine Cup, và Power Platform có thể dẫn tới lộ lọt thông tin, cho phép đối tượng tấn công leo thang đặc quyền.

- CVE-2024-38139 (Điểm CVSS: 8.7) – Xác thực sai cách trên Microsoft Dataverse cho phép đối tượng tấn công leo thang đặc quyền qua hệ thống mạng
- CVE-2024-38204 (Điểm CVSS: 7.5) - Access Control sai cách trên Imagine Cup cho phép đối tượng tấn công leo thang đặc quyền qua hệ thống mạng
- CVE-2024-38190 (Điểm CVSS: 8.6) – Thiếu ủy quyền trên Power Platform cho phép đối tượng tấn công truy cập thông tin trái phép

Đồng thời, thông tin về lỗ hổng nghiêm trọng trên Apache Solr (CVE-2024-45216, điểm CVSS: 9.8) cũng đã được công bố, lỗ hổng này có thể dẫn tới việc bỏ qua xác thực.

Nguồn: https://thehackernews.com/2024/10/critical-kubernetes-image-builder.html

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 **766** lỗ hổng, trong đó có 330 lỗ hổng mức Cao, 282 lỗ hổng mức Trung bình, 31 lỗ hổng mức Thấp và 123 lỗ hổng chưa đánh giá. Trong đó có ít nhất 131 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 GitLab, Linear eMerge và BitCoin Core, cụ thể là như sau:

- **CVE-2024-9164 (Điểm CVSS: 9.6 – Nghiêm trọng):** Lỗ hổng tồn tại trên GitLab EE cho phép đối tượng tấn công chạy pipeline trên các nhánh của dự án bất kì. Cho phép đối tượng tấn công thực thi mã từ xa, đánh cắp dữ liệu hoặc các hành vi độc hại khác nếu bị khai thác. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm đối tượng tấn công
- **CVE-2021-9441 (Điểm CVSS: 9.8 – Nghiêm trọng**): Là lỗi OS command injection tồn tại trên Linear eMerge e3-Series, cho phép đối tượng tấn công thực thi lệnh OS tùy ý thông qua tham số login_id khi gọi hàm forgot_password thông qua giao thức HTTP. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-35202 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên Bitcoin Core, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ bằng cách cho nội dung thanh toán vào thông điệp “blocktxn” không nằm trong merkle root của khối. Hiện lỗ hổng chưa có mã khai thác và chưa 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-2024-9164	- Điểm CVSS: 9.6 (Nghiêm trọng) - Ảnh hưởng: GitLab - 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-2024-9164
2	CVE-2024-9441	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Linear eMerge e3-Series - 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-2024-9441
3	CVE-2024-35202	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Bitcoin Core - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-35202
4	CVE-2024-35250	- 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-2024-35250
5	CVE-2024-30090	- Điểm CVSS: 7.0 (Cao) - Ảnh hưởng: Microsoft - 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-2024-30090

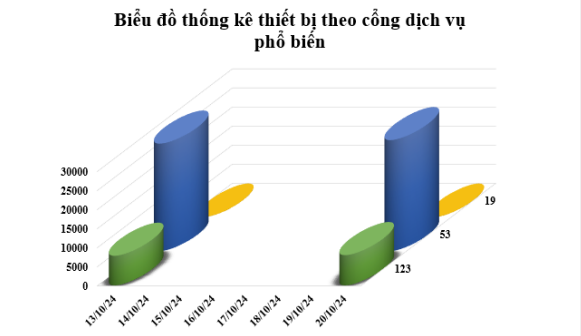
TOP 10 lỗ hổng đáng chú ý trong tuần

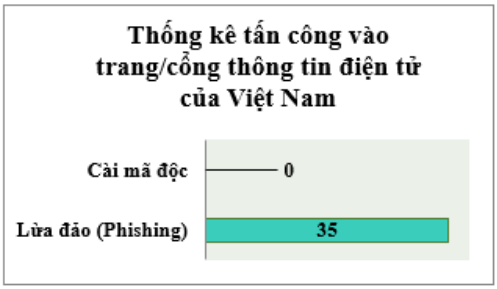
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-38200	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Microsoft Office - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công giả mạo (Spoofing) - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-38200
7	CVE-2024-9680	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Firefox - 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-2024-9680
8	CVE-2024-40711	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Veeam Backup - 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-2024-40711
9	CVE-2024-42640	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: angular-base64-upload - 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 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-2024-42640
10	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

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 **37.102** (tăng so với tuần trước **36.023**) 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.



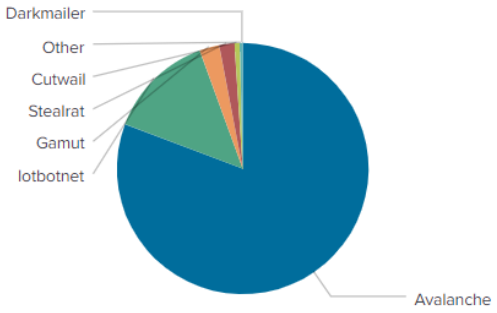


Tấn công Web

Trong tuần, có **35** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 35 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

differentia.ru	restless.su
disorderstatus.ru	api.garageserviceoperation.com
amnsreiuojy.ru	spaines.pw
atomictrivia.ru	yk37wagdg.life
hzmksreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	www.rybmqwcqup.info
restlesz.su	www.businesslunch.com
xjpakmdcfuqe.in	vhcnbcobx.com
xjpakmdcfuqe.ru	netmentdome.info
xjpakmdcfuqe.com	maxisurf.net

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **5.058** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- 190 trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- 4.868 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	www[.]ccty-ghtk[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	dichvugiaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	vietcp[.]com	Website giả mạo Dịch vụ công Quốc Gia
4	soyte[.]cc	Website giả mạo Dịch vụ công quốc gia
5	dichvucong[.]ccbcavn[.]cc	Website giả mạo Dịch vụ công quốc gia
6	dienmayxanhcenter[.]vn	Website giả mạo Điện máy xanh
7	giaohangtietkiemvn[.]website	Website giả mạo Giao hàng tiết kiệm
8	thuongmai-dientu[.]com	Website giả mạo sàn TMĐT Lazada
9	acb[.]chamsocthe-uudaikhachhang-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
10	acb[.]chamsockhachhang-uudaithetructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
11	acb[.]uudaikhachhang-chamsocthetructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
12	www[.]acb[.]uudaikhachhang-tructuyen-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
13	www[.]acb[.]chamsocthe-uudaikhachhang-tructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
14	vpbank[.]uudaikhachhang-chamsocthetructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
15	tiki886[.]vip	Website giả mạo sàn TMĐT Sendo
16	s[.]shopee[.]vn	Website giả mạo sàn TMĐT Shopee
17	sp5583p[.]com	Website giả mạo sàn TMĐT Shopee
18	https://www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
19	chinhphu[.]thongtincancuoc[.]com	Website giả mạo Văn phòng Chính phủ
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