UBND TỈNH KIÊN GIANG
SỞ Y TẾ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 2064 /SYT-VP
V/v cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép

Kiên Giang, ngày 25 tháng 6 năm 2024

Kính gửi:
- Các phòng chức năng Sở Y tế;
- Thủ trưởng các đơn vị trực thuộc Sở Y tế.
(sau đây gọi là đơn vị)

Thực hiện Công văn số 1216/STTTT-CĐS ngày 29/5/2024 của Sở Thông tin và Truyền thông về việc cảnh báo cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép.

Trong quá trình giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận các thông tin liên quan đến các chiến dịch tấn công mạng sử dụng mã độc để thực hiện các hành vi trái phép. Cụ thể, lỗ hổng an toàn thông tin trên Foxit PDF Reader đã được xác định là đang bị khai thác bởi các đối tượng tấn công để lan truyền mã độc. Đồng thời Cục An toàn thông tin cũng ghi nhận thông tin về một chiến dịch tấn công do nhóm Earth Hundun thực hiện trong năm 2024, trong đó sử dụng mã độc RAT để tiến hành các chuỗi tấn công và lan truyền mã độc vào các thiết bị khác.

(Thông tin chi tiết xem tại phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị trực thuộc Sở Y tế;

Sở Y tế yêu cầu các đơn vị triển khai thực hiện một số nội dung sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên. Chủ động theo dõi các thông tin liên quan đến chiến dịch tấn công mạng, sẵn sàng các biện pháp bảo mật để tránh nguy cơ bị tấn công.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong quá trình triển khai, thực hiện có khó khăn vướng mắc xin liên hệ Sở Y tế (qua Văn phòng gặp bà Bùi Thanh Hương, SĐT: 09453823839) để phối hợp thực hiện.

Nhận được Công văn đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

***Nơi nhận*:**
- Như trên;
- Trang VPĐT;
- Lưu: VT, bthuong.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH KIÊN GIANG

Chung Tấn Thịnh

PHỤ LỤC

THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

(Kèm theo Công văn số 2064/SYT-VP ngày 25 /6/2024 của Sở Y tế Kiên Giang)

1. Thông tin chi tiết về lỗ hổng an toàn thông tin trên Foxit PDF Reader

Gần đây, đã phát hiện hành vi sử dụng file PDF nhằm khai thác lỗ hổng trên phần mềm Foxit Reader khiến người dùng thực thi các câu lệnh độc hại trên thiết bị của mình. Hiện lỗ hổng đang được khai thác bởi nhiều nhóm tấn công trong môi trường thực tế.

Qua quá trình phân tích, các chuyên gia bảo mật đã phát hiện nhiều chủng mã độc, công cụ độc hại được sử dụng trong chuỗi lây nhiễm như: VenomRAT, Agent-Tesla, Remcos, NjRAT, NanoCore RAT, Pony, Xworm, AsyncRAT và DCRat.

Lỗ hổng trên phần mềm Foxit PDF Reader đã bị khai thác bởi nhiều nhóm tấn công khác nhau với điểm chung là mã độc được phát tán dưới dạng các file PDF độc hại. Một số chiến dịch đáng chú ý có thể kể tới là:

- Nhóm tấn công APT-C-35 (DoNot Team) sử dụng mã độc Rafel RAT để thu thập và tải về máy chủ C&C các file tài liệu, ảnh, file nén và file cơ sở dữ liệu.

- Một số đối tượng tấn công chưa xác định đã phát tán các file PDF độc hại thông qua mạng xã hội Facebook, ứng dụng Discord nhằm phát tán mã độc RAT đánh cắp dữ liệu cookies, thông tin xác thực của người dùng trên trình duyệt Google Chrome và Edge, cùng với mã độc đào tiền ảo.

- Chiến dịch sử dụng nền tảng Trello làm nơi lưu trữ để phát tán mã độc Remcos RAT nhằm vào người dùng tại Việt Nam, Hàn Quốc cùng một số quốc gia khác.

Các đơn vị có thể tải xuống các mã IOC tại https://alert.khonggianmang.vn/

Dưới đây là một số IoC được ghi nhận

(Máy chủ C&C Remcos RAT) 139.99.85[.]106:2404	(Remcos) 0ADE87BA165A269FD4C03177226A 148904E14BD328BDBB31799D2EAD 59D7C2FA
(Avict Software) 3f291d07a7b0596dcdf6f419e6b38645b 77b551a2716649c12b8706d31228d79	(Avict Software) İD02712b557a93da23bbf4207e5bc57cc 5e4e6e841653ffab59deb97b 19f214e
(PDF Exploit Builder) ac7598e2b4dd12ac584a288f528a94c48 4570582c9877c821c47789447b780ec	(FuckCrypt) 20549f237f3552570692e6e2bb31c4d2d df8133c5f59f5914522e88239370514
(FuckCrypt) 87effdf835590f85db589768b14adae2f7 6b59b2f33fae0300aef50575e6340d	(FuckCrypt) 5c42a4b474d7433bd9f1665dc914de7b3 cc7fbdb9618b0322324b534440737d7

(Python) 79e1cb66cb52852ca3f46a2089115e11f ff760227ae0ac13f128dda067675fbc	(Python) a4a8486c26c050ed3b3eb02c826b1b67e 505ada0bf864a223287d5b3f7a0cde0
(PDF) d44f161b75cba92d61759ef535596912e 1ea8b6a5a2067a2832f953808ca8609	(PDF) 9c5883cf118f1d22795f7b5661573f809 9554c5a3f78d592e8917917baa6d20f
(PDF) 2aa9459160149ecefd1c9b63420eedc7f e3a21 ae0ca3e080c93fd39fef32e9c0	(PDF) 8155a6423d64f30d2994163425d3fbe14 a52927d3616ffacea36ddc71a6af4b0
(PDF) c1436f65acbf7123d1a45b0898be69ba9 64f0c6d569aa350c9d8a5f187b3c0e7	(PDF) de8ecd738f1 f24a94aba06f19d426399bc 250cc5e7b848b2cbd92fc1d6906403
(Blank-Grabber) d2bd6a05d1e30586216e73602a053673	(Python-Stealer-Dropper) e32d2966a22243f346e06d4da5164abab

80ae66654cd0bccabb0414ef6810ab18	63c2700c905f22c09a18125ee4de559
(BAT file) eb87ec49879dc44b6794bb70bd6c706e 74694e4c2bbc1926dd4cff42e5b63cc6	(BAT file) b59ab9147214bc1682006918692febed4 ad37e1d305c5c80dc1ee461914eacd2
(APT-C-35 / DoNot Team Downloader) 4ef9133773d596d1c888b0ffe36287a81 0042172b0af0dfad8c2b0c9875d 1 c65	(APT-C-35 / DoNot Team Downloaded1) 3e9a60d5f6174bb 1 f1 c973e9466f3e70c7 4c771043ee00688e50cac5e8efe 185
(APT-C-35 / DoNot Team Uploader) 2d40e892e059850ba708f8092523efeed e759ecd6e52d8cb7752462fcdb6f715	(APT-C-35 / DoNot Team Screen) C943fe1b8e1b17ec379d33a6e5819a573 6cb5de13564f86f1d3fba320ccebaa0
(APT-C-35 / DoNot Team APK) 7f5f1586b243f477c484c34fa6243c20b 3ecf29700c6c17e23a4daf9360e2d2f	(APT-C-35 / DoNot Team APK) ecb4f5f0ee0cda289056f2f994c061d53c íbc8ac413f2ca4da8864c68İDa23f6
(APT-C-35 / DoNot Team APK) 4a7aeb6f510cf5d038e566a3ccd45e98a 46463bb67eb34012c8e64444464b081	(PDF) D5483049DC32D1A57E759839930FE 17FE31A5F513D24074710F98EC186F 06777
(PDF) 19A8201C6A3063B897D696330C1B6 0BD97914514D2AE6A6C3C1796BEC 236724A	(VBScript) 9A7F4FF5FD0A972EEDA9293727F0 EECDD7CE2CFE0A072CDF9D3402E E9C46A48E
(VBScript) D761FE4D58FE68FC95D72871429F0 FCE6055389A58F81CF0A19EB905A 96E1C38	(VBScript) B3AD75EEF9208D58A904030D44DA 22C59CE7BD47ED798B0A14B58330 A1390FE8

(VBScript) FC330BB132A345AF05FEB0D275EE EF29C7A439A04223757F33360393C	(VBScript) A334A9C1A658F4EBEF7BA336F9A2 7693030DC444509BD9FA8FDEFE8A

F975CA9	AAE3A133
(VBScript) E9BF261A779C1B3A023189BEF5095 79BAD8B496DCFE5E96C19CF8CC8 BEA48A08	(VBScript) EE42CF45FFF12BCC9E9262955470B FED810F3530E651FDDB0544562646 35D9D2
(VBScript) 1CBF897CCCC22A1E6D6A12766AD F0DCEE4C103539ADD2C10C790604 2E19519F4	(DynamicWrapperX) 4EF3A6703ABC6B2B8E2CAC3031C1 E5B86FE8B377FDE92737349EE52BD 2604379
(ShellCode) A5C9A3 518F072982404E68DC6A3D C90EDEBBF292FC1ACA6962B6CCF 64F4FE28C	0

2. Thông tin chi tiết về chiến dịch tấn công của nhóm Earth Hundun

Nhóm tấn công APT Earth Hundun nhằm vào khu vực Châu Á Thái Bình Dương sử dụng mã độc Waterbear và biến thể mới nhất Deuterbear. Mã độc Deuterbear lần đầu được ghi nhận sử dụng vào tháng 10/2022.

Mã độc Deuterbear RAT đã được cải thiện khả năng bằng cách thu gọn lại chỉ còn 20 câu lệnh, có khả năng nhận nhiều plugin hơn để cải thiện tính linh động, bổ sung các chức năng cho phép điều khiển thiết bị người dùng dễ hơn.

Các đơn vị có thể tải xuống các mã IOC tại https://alert.khonggianmang.vn/

Dưới đây là số IOC được ghi nhận:

* .quadrantbd[.]com	*.taishanlaw[.]com
*.bakhell[.]com	*.gelatosg[.]com
*.operatida[.]com	*.randaln[.]com
* .nestnewhome[.]com	*.dailteeau[.]com
*.lucashnancy[.]com	*.ccarden[.]com

*.availitond[.]com	*.gayionsd[.]com
*.rchitecture[.]org	*.operatida[.]com
*.centralizebd[.]com	609120ab45745bcfe8abc244ea1501 ef56 3cb666abd9d730413c3986a76fb23d
88336746f2cf1034871c4ee334fae0d30c 3eb101 df6f3f1c94c777639293a031	3ecbca7bf2e4557e92595fe23872658bc3 337e6f77a3aff02fb7b460272de7f4
d4b5127988fde3704193a30840e991 dc7 45aea051d1551c7cb6f55853c8cb9da	974c407dd918ccba245da0fb9d5a68f12 3c78aacfa85cdaba2271d6ad81380ae
3d8512a513e5f94ce49a742ae3e485377 5f05d7481b29bfacef4316d7ba3bde2	057a0e0f522cc217ba8754abbb67f8a667 c0054fe0dcdaf01 f4930d75cd667cc
31c76585ea703f96c95efab0778f599d8d c5c26eea5d155ce24f614e6bfe9e8c	0

3. Tài liệu tham khảo

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://www.trendmicro.com/en_us/research/24/e/earth-hundun-2.html

SỞ Y TẾ KIÊN GIANG
TRUNG TÂM Y TẾ GIANG THÀNH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do - Hạnh phúc

PHIẾU GIẢI QUYẾT VĂN BẢN ĐẾN

Số: 2064 /SYT - VP ngày, 25 tháng 6 năm 2024

.....

.....

.....

.....

.....

1. Ý kiến của lãnh đạo cơ quan, tổ chức

- Giao đơn vị, cá nhân chủ trì; TCHC

- Giao các đơn vị, cá nhân tham gia phối hợp giải quyết văn bản đến (nếu có);

.....

.....

- Thời hạn giải quyết đối với mỗi đơn vị, cá nhân (nếu có);.....

.....

- Ngày,.....tháng.....năm.....cho ý kiến phân phối, giải quyết.....

Trần Thị Thu Liệt

.....

.....

2. Ý kiến của lãnh đạo Khoa, Phòng

- Giao cho cá nhân; thời hạn giải quyết đối với cá nhân (nếu có);

.....

.....

-Ngày,... tháng,.....năm.....cho ý kiến.....

.....

.....

3. Ý kiến đề xuất của người giải quyết.

- Ý kiến đề xuất giải quyết văn bản đến của cá nhân;

.....

.....

- Ngày,..... tháng,..... năm..... đề xuất ý kiến.....

.....

.....