UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 1496/STTTT-IOC
V/v cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép

Thừa Thiên Huế, ngày 29 tháng 5 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN.

Sở Thông tin và Truyền thông nhận được Công văn số 950/CATTT-NCSC ngày 27/05/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông Về việc cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép.

Cục An toàn thông tin, 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 các hệ thống thông tin, hệ thống mạng diện rộng của tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

1. Triển khai 02 giải pháp đảm bảo an toàn thông tin cho 100% các máy tính tại đơn vị: Giải pháp phòng, chống mã độc tập trung Bkav Endpoint tại Công văn số 639/STTTT-IOC ngày 29/3/2022; Giải pháp phát hiện và chống tấn công có chủ đích Viettel Endpoint tại Công văn số 1660/STTTT-IOC ngày 22/7/2022 của Sở TTTT;

2. Chú ý cảnh giác thư điện tử không rõ nguồn gốc, thư có các liên kết (link) hoặc tập tin đính kèm lạ, có dấu hiệu khả nghi. Cần lập tức chuyển các thư này đến địa chỉ tiepnhan@thuathienhue.gov.vn để bộ phận kỹ thuật hỗ trợ kiểm

tra, ngăn chặn và xử lý, tránh phát tán thư điện tử có dấu hiệu khả nghi đến người sử dụng khác;

3. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ hãng nhằm thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công.

4. 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 Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng;

5. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông: Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh – Sở Thông tin và Truyền thông:

- đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759; email: hdky.stttt@thuathienhue.gov.vn

- đ/c La Thức; điện thoại: 0772 428 218; email: lthuc.stttt@thuathienhue.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- Cục ATTT (để bc);
- Công an tỉnh (để p/h);
- BGĐ Sở;
- P.CNTT, HueIOC;
- Lưu: VT.

GIÁM ĐỐC

Nguyễn Xuân Sơn

Phụ lục

THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

(Kèm theo Công văn số /STTTT-IOC ngày /05/2024 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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) 0ADE87BA165A269FD4C03177226A148904E14BD328BDBB31799D2EAD59D7C2FA
(Avict Software) 3f291d07a7b0596dcdf6f419e6b38645b77b551a2716649c12b8706d31228d79	(Avict Software) f002712b557a93da23bbf4207e5bc57cc5e4e6e841653ffab59deb97b19f214e
(PDF Exploit Builder) ac7598e2b4dd12ac584a288f528a94c484570582c9877c821c47789447b780ec	(FuckCrypt) 20549f237f3552570692e6e2bb31c4d2ddf8133c5f59f5914522e88239370514
(FuckCrypt) 87effdf835590f85db589768b14adae2f76b59b2f33fae0300aef50575e6340d	(FuckCrypt) 5c42a4b474d7433bd9f1665dc914de7b3cc7fbdb9618b0322324b534440737d7
(Python) 79e1cb66cb52852ca3f46a2089115e11fff760227ae0ac13f128dda067675fbc	(Python) a4a8486c26c050ed3b3eb02c826b1b67e505ada0bf864a223287d5b3f7a0cde0
(PDF) d44f161b75cba92d61759ef535596912e1ea8b6a5a2067a2832f953808ca8609	(PDF) 9c5883cf118f1d22795f7b5661573f8099554c5a3f78d592e8917917baa6d20f
(PDF) 2aa9459160149ecefd1c9b63420eedc7fe3a21ae0ca3e080c93fd39fef32e9c0	(PDF) 8155a6423d64f30d2994163425d3fbe14a52927d3616ffacea36ddc71a6af4b0
(PDF) c1436f65acbf7123d1a45b0898be69ba964f0c6d569aa350c9d8a5f187b3c0e7	(PDF) de8ecd738f1f24a94aba06f19d426399bc250cc5e7b848b2cbd92fc1d6906403

(Blank-Grabber) d2bd6a05d1e30586216e73602a05367380ae66654cd0bccabb0414ef6810ab18	(Python-Stealer-Dropper) e32d2966a22243f346e06d4da5164ababb63c2700c905f22c09a18125ee4de559
(BAT file) eb87ec49879dc44b6794bb70bd6c706e74694e4c2bbc1926dd4cff42e5b63cc6	(BAT file) b59ab9147214bc1682006918692febed4ad37e1d305c5c80dc1ee461914eacd2
(APT-C-35 / DoNot Team Downloader) 4ef9133773d596d1c888b0ffe36287a810042172b0af0dfad8c2b0c9875d1c65	(APT-C-35 / DoNot Team Downloaded1) 3e9a60d5f6174bb1f1c973e9466f3e70c74c771043ee00688e50cac5e8efe185
(APT-C-35 / DoNot Team Uploader) 2d40e892e059850ba708f8092523efeede759ecd6e52d8cb7752462fcdb6f715	(APT-C-35 / DoNot Team Screen) c943fe1b8e1b17ec379d33a6e5819a5736cb5de13564f86f1d3fba320ccebaa0
(APT-C-35 / DoNot Team APK) 7f5f1586b243f477c484c34fa6243c20b3ecf29700c6c17e23a4daf9360e2d2f	(APT-C-35 / DoNot Team APK) ecb4f5f0ee0cda289056f2f994c061d53cfbc8ac413f2ca4da8864c68f0a23f6
(APT-C-35 / DoNot Team APK) 4a7aeb6f510cf5d038e566a3ccd45e98a46463bb67eb34012c8e64444464b081	(PDF) D5483049DC32D1A57E759839930FE17FE31A5F513D24074710F98EC186F06777
(PDF) 19A8201C6A3063B897D696330C1B60BD97914514D2AE6A6C3C1796BEC236724A	(VBScript) 9A7F4FF5FD0A972EEDA9293727F0EECDD7CE2CFE0A072CDF9D3402EE9C46A48E
(VBScript) D761FE4D58FE68FC95D72871429F0FCE6055389A58F81CF0A19EB905	(VBScript) B3AD75EEF9208D58A904030D44DA22C59CE7BD47ED798B0A14B583

A96E1C38	30A1390FE8
(VBScript) FC330BB132A345AF05FEB0D275E EEF29C7A439A04223757F33360393 CF975CA9	(VBScript) A334A9C1A658F4EBEF7BA336F9A 27693030DC444509BD9FA8FDEFE8 AAAE3A133
(VBScript) E9BF261A779C1B3A023189BEF509 579BAD8B496DCFE5E96C19CF8CC 8BEA48A08	(VBScript) EE42CF45FFF12BCC9E9262955470 BFED810F3530E651FDDB05445626 4635D9D2
(VBScript) 1CBF897CCCC22A1E6D6A12766A DF0DCEE4C103539ADD2C10C7906 042E19519F4	(DynamicWrapperX) 4EF3A6703ABC6B2B8E2CAC3031C 1E5B86FE8B377FDE92737349EE52 BD2604379
(ShellCode) A5C9A3518F072982404E68DC6A3D C90EDEBBF292FC1ACA6962B6CC F64F4FE28C	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	609120ab45745bcfe8abc244ea1501ef563cb666abd9d730413c3986a76fb23d
88336746f2cf1034871c4ee334fae0d30c3eb101df6f3f1c94c777639293a031	3ecbca7bf2e4557e92595fe23872658bc3337e6f77a3aff02fb7b460272de7f4
d4b5127988fde3704193a30840e991dc745aea051d1551c7cb6f55853c8cb9da	974c407dd918ccba245da0fb9d5a68f123c78aacfa85cdaba2271d6ad81380ae
3d8512a513e5f94ce49a742ae3e4853775f05d7481b29bfacef4316d7ba3bde2	057a0e0f522cc217ba8754abbb67f8a667c0054fe0dcdaf01f4930d75cd667cc
31c76585ea703f96c95efab0778f599d8dc5c26eea5d155ce24f614e6bfe9e8c	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