UBND THÀNH PHỐ BẮC KẠN
PHÒNG VĂN HÓA VÀ THÔNG TIN

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

Số: 198 /VHTT
V/v cảnh báo chiến dịch tấn công mạng

TP. Bắc Kạn, ngày 13 tháng 9 năm 2024

Kính gửi:
- Ủy ban MTTQ và các đoàn thể thành phố;
- Các phòng, ban, đơn vị thành phố;
- Ủy ban nhân dân xã, phường;
- Các trường TH, THCS, TH&THCS thuộc thành phố.

Thực hiện Công văn số 1299/STTTT-CNTT-BCVT ngày 12/9/2024 của Sở Thông tin và Truyền thông tỉnh Bắc Kạn về việc cảnh báo chiến dịch tấn công có chủ đích vào các hệ thống quan trọng, theo đó, Cục An toàn Thông tin, Bộ Thông tin và Truyền gia ghi nhận các chiến dịch tấn công nhắm vào các tổ chức và doanh nghiệp với mục tiêu chính là tấn công mạng, đánh cắp thông tin và phá hoại hệ thống.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, Phòng Văn hoá và Thông tin thành phố Bắc Kạn đề nghị các cơ quan, đơn vị tăng cường giám sát hoạt động của các hệ thống thông tin 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 *(chi tiết về mã độc tại phụ lực gửi kèm)*.

Với nội dung trên đề nghị các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:
Gửi bản điện tử:
- Như trên;
- CT, PCT UBND TP (Ô. Trưởng);
- Lưu: VHTT.

TRƯỞNG PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG VĂN HÓA VÀ THÔNG TIN
TP. BẮC KẠN T. BẮC KẠN

Vũ Thị Kim Quỳnh

Phụ lục I

THÔNG TIN VỀ CÁC LỖ HỔNG PAN-OS

(Kèm theo Công văn số: /VHTT ngày 13/9/2024 của Phòng văn hoá và Thông tin thành phố Bắc Kạn)

1. Thông tin chi tiết các chiến dịch tấn công

Trong thời gian gần đây, Trung tâm Giám sát an toàn không gian mạng quốc gia ghi nhận các chiến dịch tấn công nhắm vào các tổ chức và doanh nghiệp với mục tiêu chính là tấn công mạng, đánh cắp thông tin và phá hoại hệ thống.

Mallox Ransomware, nổi lên từ năm 2023 hoạt động dưới dạng RaaS (Ransomware as a Service), cho phép các cuộc tấn công trên phạm vi toàn cầu, đặc biệt tại Brazil, Việt Nam và Trung Quốc. Mallox lây nhiễm qua việc khai thác lỗ hổng phần mềm và brute force trên máy chủ MS SQL hoặc PostgreSQL, sau đó triển khai mã độc như Remcos RAT hoặc bộ tải .NET để tải mã độc giai đoạn tiếp theo. Các phiên bản mới đã tối ưu hóa mã hóa bằng AES-256 và ECC, đồng thời tránh mã hóa trên các hệ thống dùng ngôn ngữ của các nước thuộc khối Liên Xô cũ.

Nhóm APT Lazarus đã phát tán mã độc thông qua phần mềm họp video giả mạo tên FCCCall trong các chiến dịch tấn công chuyên gia blockchain và dự án web game. Lazarus tiếp cận mục tiêu qua các nền tảng tìm kiếm việc làm như LinkedIn và sử dụng Telegram để trích xuất dữ liệu. Mã độc BeaverTail và InvisibleFerret được sử dụng để đánh cắp thông tin từ trình duyệt, ví tiền ảo và ứng dụng quản lý mật khẩu, cũng như cấu hình AnyDesk truy cập từ xa. Mã độc này còn được nhúng vào các dự án Node.js trên GitHub, Gitlab để ẩn mã độc và tránh bị phát hiện.

Nhóm APT Stately Taurus (Mustang Panda) đã khai thác lỗ hổng trên Visual Studio Code, sử dụng tính năng reverse shell để thực thi mã từ xa và tải xuống payload độc hại. Nhóm sử dụng OpenSSH để chuyển file, quét mạng bằng SharpNBTScan và nén dữ liệu qua Listeners.bat trước khi trích xuất lên Dropbox. Các chuyên gia cũng phát hiện sự tham gia của mã độc ShadowPad, gợi ý khả năng hợp tác giữa hai nhóm tấn công.

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

Một số IoC liên quan đến các tấn công gần đây:

Chiến dịch tấn công liên quan đến mã độc Mallox ransomware

9b772efb921de8f172f21125dd0e0ff7	a8e214683307adaff39783dc656b398a
e713f05a62914496eef512a93a611622	79b60f8b5052a9d4cc0c92c2cdc47485
3829a09bca120206883539eb33d55311	3762f98a55f0ec19702f388fc0db74e2

ac1a255e5c908f12ef68a45fc0043b16	16e708876c32ff56593ba00931e0fb67
b1b42fa300d8f43c6deb98754caf0934	b13a1e9c7ef5a51f64a58bae9b508e62
6bd93817967cdb61e0d7951382390fa0	e98b3a8d2179e0bd0bebba42735d11b7
c494342b6c84f649dece4df2d3ff1031	98c7f6b6ddf6a01adb25457e9a3c52b8
d32a3478aad766be96f0cdbda1f10091	whyers.io%2FQWEwqdsvsf%2Fap.php
91.215.85.142%2FQWEwqdsvsf%2Fap.php	0

Nhóm APT Lazarus sử dụng ứng dụng Windows giả mạo nền tảng họp video để phát tán nhiều chủng mã độc

23.106.253[.]194	45.61.129[.]255	45.61.130[.]0
45.61.131[.]218	45.61.160[.]14	45.61.169[.]187
45.140.147[.]208	67.203.7[.]171	67.203.7[.]245
77.37.37[.]81	91.92.120[.]135	95.164.17[.]24
144.172.74[.]48	144.172.79[.]23	147.124.212[.]89
147.124.213[.]11	147.124.213[.]29	147.124.212[.]146
147.124.214[.]129	147.124.214[.]131	147.124.214[.]237
167.88.36[.]13	167.88.168[.]152	167.88.168[.]24
172.86.97[.]80	172.86.98[.]143	172.86.98[.]240
172.86.123[.]35	173.211.106[.]101	185.235.241[.]208
blocktestingto[.]com	de.ztec[.]store:8000	hxxp://freeconference[.]io
hxxp://mirotalk[.]net	hxxp://ipcheck[.]cloud	hxxp://regioncheck[.]net

Nhóm APT Trung Quốc khai thác VSCode để tấn công nhằm vào các tổ chức tại Châu Á

506fc87c8c96fef1d2df24b0ba44c8116a9001ca5a7d7e9c01dc3940a664acb0

aa2c0de121ae738ce44727456d97434faff21fc69219e964e1e2d2f1ca16b1c5
8fdac78183ff18de0c07b10e8d787326691d7fb1f63b3383471312b74918c39f
39ceb73bcfd1f674a9b72a03476a9de997867353172c2bf6dde981c5b3ad512a
0f11b6dd8ff972a2f8cb7798b1a0a8cd10afadcea201541c93ef0ab9b141c184
456e4dae82a12bcda0506a750eac93bf79cc056b8aad09ec74878c90fd67bd8f
bdadcd2842ed7ba8a21df7910a0acc15f8b0ca9d0b91bebb49f09a906ae217e6
216.83.40[.]84
185.132.125[.]72

2. Tài liệu tham khảo

https://securelist.com/mallox-ransomware/113529/

https://www.group-ib.com/blog/apt-lazarus-python-scripts/

https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/