BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 124 /TTCNTT-KTHT
V/v nguy cơ tấn công APT vào các cơ quan tổ chức Việt Nam

Hà Nội, ngày 11 tháng 05 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ

Theo Công văn số 324/CATTT-NCSC ngày 15/05/2020 của Cục An toàn thông tin về việc nguy cơ tấn công APT vào các cơ quan tổ chức Việt Nam, thời gian gần đây, lợi dụng tình hình dịch bệnh COVID-19, nhiều nhóm APT (tin tặc) đang tích cực hoạt động, để thực hiện tấn công vào hệ thống thông tin của nhiều quốc gia trên thế giới, trong đó có Việt Nam.

Các nhóm tin tặc này vẫn bắt đầu cuộc tấn công bằng thủ đoạn đính kèm mã khai thác điểm yếu, lỗ hổng vào các tập tin tài liệu và phát tán tập tin này qua thư điện tử. Tuy nhiên tài liệu lợi dụng để phát tán mã độc ở mỗi thời điểm thường được lựa chọn kỹ lưỡng, và là tài liệu được nhiều người quan tâm hoặc người dùng mục tiêu quan tâm: văn bản, tài liệu của các cơ quan tổ chức, gần đây là các tài liệu liên quan đến phòng chống dịch bệnh COVID-19.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của quý đơn vị, Trung tâm Công nghệ thông tin đề nghị quý đơn vị thực hiện:

1. Kiểm tra, rà soát, đổi mật khẩu các tài khoản có quyền quản trị hệ thống, tài khoản truy cập từ xa (VPN, SSH…), tài khoản người dùng.

2. Kiểm tra, rà soát, cập nhật và khắc phục các lỗ hổng bảo mật trên tất cả các hệ thống bao gồm cả các máy tính cán bộ nhân viên sử dụng để làm việc, đặc biệt lưu ý các lỗ hổng đã và đang bị lợi dụng để khai thác cài cắm mã độc vào máy tính người dùng.

3. Cập nhật dấu hiệu cho các giải pháp bảo mật, để giám sát, phát hiện và ngăn chặn sớm các nguy cơ tấn công mạng nguy hiểm. Tham khảo thông tin kỹ thuật liên quan đến các nhóm APT trong phụ lục kèm theo.

4. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị tấn công liên quan đến các nhóm APT.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VP, KTHT

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Ký bởi: Trung tâm Công nghệ thông tin
Cơ quan: Bộ Khoa học và Công nghệ
Ngày ký: 11.05.2020 10:27:43 +07:00

Hà Quốc Trung

Phụ lục 1
Một số nhóm APT có mục tiêu tấn công vào Việt Nam
(kèm theo Công văn số /TTCNTT-KTHT ngày / /2020)

STT	Tên nhóm APT	Mô tả chung
1	Goblin Panda	Còn gọi là Cycldek, Hellsing, APT27, 1937CN, hoạt động mạnh từ năm 2013-2018, được phát hiện từ năm 2010. Tấn công vào các lĩnh vực quốc phòng, năng lượng và chính phủ, nhằm mục tiêu các nước Đông Nam Á như Lào, Philippines, Thailand, Vietnam (mục tiêu chính là Lào và Việt Nam)
2	Mustang Panda	Có hoạt động từ tháng 6 năm 2018. Tấn công vào Trung tâm phi lợi nhuận Trung Quốc, đảng chính trị Việt Nam, cư dân Đông Nam Á và các quốc gia khác như Đức, Mông Cổ, Myanmar, Pakistan, Việt Nam.
3	Gothic Panda	Còn gọi là APT03, Boyusec, UPS, Gothic Panda, Tg-0110. Xuất hiện từ năm 2009, APT03 khai thác lỗ hổng zero-day trên các trình duyệt : Internet Explorer, Firefox, Adobe Flash Player.

Phụ lục 2
Danh sách lỗ hổng được các nhóm APT tận dụng để khai thác.
(kèm theo Công văn số /TTCNTT-KTHT ngày / /2020)

STT	Lỗ hổng	Mô tả
1	CVE-2012-0158	Lỗ hổng trong Microsoft Windows Common Controls cho phép kẻ tấn từ xa thực thi mã tùy ý. Thành phần này đều có trong Microsoft Windows, Internet Explorer, Microsoft .NET Framework, Microsoft Office, Microsoft Server Software, Microsoft SQL Server, Microsoft Developer Tools, and Microsoft Forefront United Access Gateway
2	CVE-2017-11882	Lỗ hổng trong Microsoft Office cho phép chèn và thực thi mã lệnh
3	CVE-2018-0802	Lỗ hổng trong Microsoft Office cho phép chèn và thực thi mã lệnh
4	CVE-2017-0199	Lỗ hổng trong Microsoft Office và Wordman cho phép kẻ tấn thực thi mã lệnh từ xa từ đó kiểm soát hệ thống.
5	CVE-2015-3113	Lỗ hổng trong Adobe Flash Player trên Windows và OS cho phép kẻ tấn công từ xa thực thi mã tùy ý
6	CVE-2019-0703	Lỗ hổng trên Windows SMB Server cho phép đối tượng tấn công thu thập thông tin
7	CVE-2017-0143	Lỗ hổng Microsoft Windows cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa
8	CVE-2010-3962	Lỗ hổng trong Microsoft Internet Explorer cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa sử dụng CSS
9	CVE-2014-1776	Lỗ hổng trong Microsoft Internet Explorer cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.
10	CVE-2015-6585	Lỗ hổng trong bộ xử lý Hangul Word (HWP) cho phép kẻ tấn từ xa thực thi mã tùy ý thông qua một heap và tệp HWPX.
11	CVE-2018-20250	Lỗ hổng trong WinRAR, lỗ hổng truyền tải đường dẫn khi tạo trường tên tệp theo định dạng ACE.
12	CVE-2016-0034	Lỗ hổng Microsoft Silverlight cho phép kẻ tấn công từ xa thực thi mã tùy ý.
13	CVE-2018-4878	Lỗ hổng tồn tại trong Adobe Plash Player 28.0.0.137 cho phép kẻ tấn công chiếm quyền kiểm soát hệ thống bị xâm nhập.

14	CVE-2017-8291	Lỗ hổng trong Artifex Ghostscript cho phép bỏ qua –dSAFER và thực thi lệnh từ xa thông qua nhầm lẫn loại .rsdparams với chuỗi con “/OutputFile.
15	CVE-2017-0144 CVE-2017-0145	Lỗ hổng trong Windows SMB cho phép kẻ tấn công thực thi mã tùy ý từ xa.
16	CVE-2017-7269	Lỗ hổng trong Microsoft (IIS) 6.0 cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua một tiêu đề bắt đầu bằng "If: <http: //" trong yêu cầu PROPFIND.

Phụ lục 3
Thông tin IoC liên quan đến các nhóm APT

(kèm theo Công văn số /TTCNTT-KTHT ngày / /2020)

Loại IoC	Giá trị	Ghi chú
IP/Domain	tintuc.mattrantoquocvnnhanoihcm.com static.bambooairwaysshy.com 160.20.147.206 92.38.135.81	
IP/Domain	skypechatvideo.online	
IP/Domain	mine.remaariegarcia.com egg.stralisemariegar.com api.anaehler.com cloud.anofrio.com video.viodger.com term.ursulapaulet.com inc.graceneufville.com log.osloger.biz file.log4jv.info news.sqllitlever.info us.jaxonsorensen.club staff.kristianfiedler.club bit.catalinabonami.com hr.halettebiermann.com cyn.ettebiermahalet.com	

Ghi chú: *Số lượng IoC là rất nhiều và thay đổi thường xuyên, nên sẽ được Trung tâm NCSC, Cục An toàn thông tin cập nhật thường xuyên thông qua Hệ thống Phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam.*