UBND TỈNH BẮC NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
Số: 420 /STTTT-CNTT
V/v cảnh báo tấn công có chủ đích sử dụng mã độc

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

Bắc Ninh, ngày 30 tháng 6 năm 2017

SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG T. BẮC NINH
ĐẾN Số:
Ngày: 3/7/2017
Chuyển: TTCNTT.

Kính gửi:
- Các Sở, ban, ngành trực thuộc UBND tỉnh;
- UBND các huyện, thị xã, thành phố.

— VPS.

Sở Thông tin và Truyền thông nhận được Công văn số 172/CNTTGSM-ANM ngày 27/6/2017 của Trung tâm Công nghệ thông tin và giám sát an ninh mạng – Ban Cơ yếu Chính phủ về việc tấn công có chủ đích sử dụng mã độc, nhằm vào các cơ quan chính phủ để đánh cắp thông tin nhạy cảm, đặc biệt là các dữ liệu liên quan đến việc tổ chức diễn đàn hội nghị APEC.

Để giảm thiểu rủi ro về an toàn thông tin, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị trên địa bàn tỉnh thực hiện và chỉ đạo các cơ quan, đơn vị trực thuộc khẩn trương tiến hành rà soát, thực hiện các nội dung hướng dẫn tại công văn số 172/CNTTGSM-ANM *(có văn bản kèm theo)*.

Trong quá trình sử dụng Internet, nếu nhận được các email lạ có đính kèm theo các file nghi ngờ là mã độc, đề nghị không mở file đính kèm để tránh bị nhiễm mã độc và gửi chuyển tiếp về địa chỉ email ttcntttt.stttt@bacninh.gov.vn hoặc liên hệ đồng chí Lại Hữu Dương, Phó Giám đốc Trung tâm CNTT&TT; SĐT di động: 0912.339.623; CĐ: 0222.3875606 để Sở tổng hợp, phân tích và xử lý.

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị trên địa bàn tỉnh được biết và nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc, các Phó Giám đốc Sở (b/c);
- Các phòng, đơn vị thuộc Sở (t/h);
- Phòng VHTT các huyện, thị xã, thành phố (đ/b);
- Lưu: VT, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH BẮC NINH

Nguyễn Văn Hào

Người ký: Sở Thông tin và Truyền thông
Email: stttt@bacninh.gov.vn
Cơ quan: Tỉnh Bắc Ninh
Thời gian ký: 30.06.2017 14:18:50 +07:00

BAN CƠ YẾU CHÍNH PHỦ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ GIÁM SÁT AN NINH MẠNG

Số: 172/CNTTGSM-ANM
V/v tấn công có chủ đích sử dụng mã độc

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

Hà Nội, ngày 27 tháng 6 năm 2017

Kính gửi:
- Trung tâm CNTT Văn phòng Trung ương Đảng;
- Vụ Tổ chức - Hành chính Văn phòng Chủ tịch nước;
- Trung tâm tin học Văn phòng Quốc hội;
- Cổng thông tin điện tử Văn phòng Chính phủ;
- Trung tâm tin học Văn phòng Chính phủ;
- Trung tâm thông tin Bộ Ngoại giao;
- Cục CNTT Bộ Tư Pháp;
- Sở TTTT Thành phố Đà Nẵng;
- Văn phòng UBND TP Hồ Chí Minh;
- Sở TTTT Bắc Ninh;
- Sở TTTT Thái Bình;
- Cục TTKH và CNQG - Bộ KH-CN;
- Sở TTTT Hà nội;
- Trung tâm TT Bộ Nông nghiệp;
- Trung tâm CNTT Bộ Giao thông Vận tải;
- Tổng Công ty quản lý bay Việt Nam; Hãng Hàng Không VietNam Airline.

Theo cảnh báo của hãng Checkpoint và qua theo dõi, phân tích của Trung tâm CNTT và Giám sát An ninh mạng Ban Cơ yếu Chính phủ, trong thời gian gần đây (3-6/2017) xuất hiện một loại mã độc mới có tên Trojan.Farfli. Mục tiêu của loại mã độc này là nhằm vào các cơ quan chính phủ để đánh cắp thông tin nhạy cảm, đặc biệt là các dữ liệu liên quan đến việc tổ chức diễn đàn hội nghị APEC. Mã độc được đính kèm trong các file văn bản có tên "Hợp tác kinh tế Châu Á Thái Bình Dương năm 2017 – 2020 (mard).doc; APEC – SMEWG Strategicpla 2017-2020.doc; APEC Strategic Plan 2017-2020(final).doc và gửi qua đường email, khi người dùng mở email Trojan.Farfli sẽ xâm nhập, nằm vùng và đánh cắp các tài liệu, thông tin trong hệ thống máy tính bị lây nhiễm loại mã độc này, chi tiết về loại mã độc này có Phụ lục kèm theo.

Trung tâm Công nghệ thông tin và Giám sát an ninh mạng thông báo cho các cơ quan được biết và cảnh giác với loại mã độc trên. Nếu nhận được email trên hoặc email có dạng như trên thì tuyệt đối không được mở file đính kèm theo email để tránh bị nhiễm virus. Quý cơ quan có thể download công cụ để kiểm tra hệ thống xem có bị nhiễm loại mã độc trên tại địa chỉ htttp://antoanthongtin.vn/.

Trong quá trình sử dụng Internet nếu nhận được các email lạ có đính kèm theo các file nghi ngờ là mã độc, đề nghị không mở file đính kèm để tránh bị nhiễm mã độc và gửi chuyển tiếp (forward) về địa chỉ email: anm@bcy.gov.vn để Trung tâm phân tích và xử lý./

Nơi nhận:
- Như trên;
- Lãnh đạo ban (để b/c);
- Lưu: VT; P.ĐGANM; Th03.

GIÁM ĐỐC

BAN CƠ YẾU CHÍNH PHỦ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ GIÁM SÁT AN NINH MẠNG

Trần Đức Sự

PHỤ LỤC

PHÂN TÍCH SƠ BỘ MÃ ĐỘC TẤN CÔNG CÓ CHỦ ĐÍCH VÀO CÁC CƠ QUAN CHÍNH PHỦ ĐỂ KHAI THÁC THÔNG TIN VỀ HỘI NGHỊ APEC

Trojan.Farfli được đính kèm vào các bản world chứa trong các email giả mạo cố tình truy cập và đánh cắp thông tin vào máy bị nhiễm.

Activity Set	Sample MD5	Filename	C&C Domain (IP Address)	Suspected Target
1	293b297852eed027 26be916bc43c81f4	KingKong.dll	Msdns.otzo.com (45.121.146.26)	VN Gov't Agency, VN ISP
	77d13e9f04dec82e6 70a5afda0f2f148	KingKong.dll	ftp.chinhphu.ddns.ms (45.121.146.26)	Suspected VN User
	5ca90fcaf73159d235 5d1bbfdaf37257	KingKong.dll	www.microsoft.https443.org (45.121.146.26)	Suspected VN User
2	5835955708c171503 b7ee6b75dd18807	Unknown	• www.winupdate.ddns.ms • microsoft.serveusers.com (121.126.31.67)	Unknown
	2e5020bfba812f6a8 d678bcc2f456831	1.bin	• www.winupdate.ddns.ms • microsoft.serveusers.com (121.126.31.67)	Unknown
	9d1af0141067250fc efefeb230985e0c	Kế hoạch về việc công khai Bản kê tài sản, thu nhập năm 2014.ppsx	• www.winupdate.ddns.ms • microsoft.serveusers.com (121.126.31.67)	Suspected VN User
3	5df67ce8487d3e995 0d669a9052c4f55	RunningDll.dll	web.jjcwa.com (210.56.63.61)	Hong Kong lawmaker
	e87b93e2af67be2c1 e41b1228e0f3de9	Unknown	• web.jjcwa.com • web.pkuch.com (210.56.63.61)	Unknown

Bảng 1: Các mẫu liên quan đến các hoạt động tấn công mã độc

Mục tiêu loại mã độc này tìm kiếm và đánh cắp là các nội dung có liên quan đến các đề xuất mà chính phủ Việt Nam đưa ra đề xuất trong diễn đàn hội nghị APEC sắp tới.

Vào các ngày 6,7,14 tháng 3 năm 2017 qua theo dõi đã phát hiện một máy chủ của cơ quan thuộc chính phủ bị tấn công bằng mã độc Trojan.Farfli gồm các đặc điểm sau:

- Tập tin word có tên "Hợp tác kinh tế Châu Á Thái Bình Dương năm 2017 – 2020 (mard).doc" được gửi đính kèm trong một email giả mạo. Mẫu mã độc (MD5: 293b297852eed02726be916bc43c81f4) có thư viện được đặt tên theo bộ phim nổi tiếng Kingkong: CSIDL_COMMON_APPDATA \ basekst \ kingkong.dll, được công chiếu vào cùng thời điểm.

Tên miền ra lệnh và điều khiển (C&C) là msdns.otzo.com, phân giải ra có địa chỉ IP là 45.121.146.26. Địa chỉ IP này được đăng ký bởi TheGigabit, một nhà cung cấp Hosting tại Malaysia.

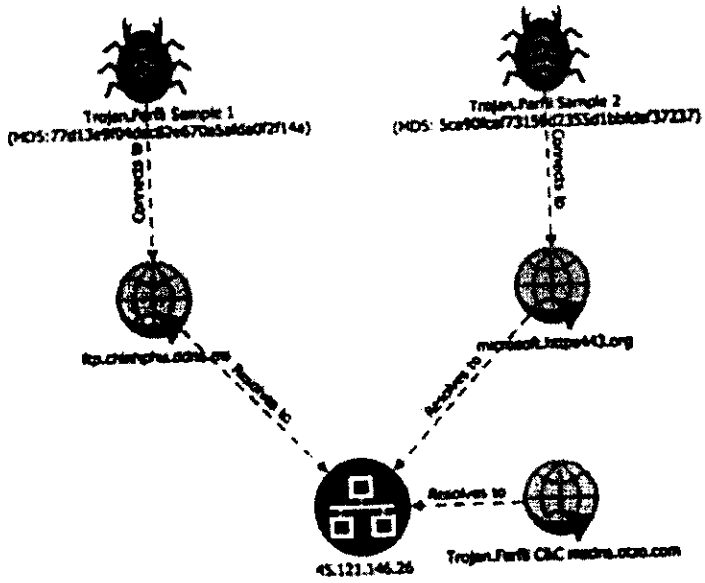
Ngoài ra còn phát hiện địa chỉ từ Việt Nam gửi 2 tài liệu vào ngày 23 và 28 tháng 3 năm 2017 như sau:

- APEC-SMEWG Strategic Plan 2017-2020.doc (MD5: 2030ce7a53ac9846086f60c691b3f9db)

- APEC Strategic Plan 2017-2020(final).doc (MD5: bc41f57ea481c94c97e8ff23735e141b)

Khi mở các tập tin này thì đồng thời sẽ kích hoạt mã độc và mã độc này sẽ khai thác lỗ hổng có định danh CVE2014-4114

Khi kiểm tra hai mẫu trên, phát hiện có mã độc kết nối tới một địa chỉ website tại Trung Quốc http://ip138.com trước khi có kết nối với máy chủ C&C: ftp.chinhphu.ddns.ms và www.microsoft.https443.org. Cả hai tên miền phân giải ra địa chỉ IP đều là 45.121.146.26 – giống với địa chỉ sử dụng trong hành vi của Trojan.Farfli ngày 6, 7 và 14 tháng 3/2017 (hình 1).



Hình 1. Kết nối C&C giữa các mẫu Trojan.Farfli

Cách thức hoạt động của mã độc Trojan.Farfli như sau:

Khi nhiễm vào máy tính, Trojan.Farfli sẽ ghi vào những vị trí sau của registry:

- %ALLUSERSPROFILE%\BaseKst\KingKong.dll
- %ALLUSERSPROFILE%\BaseKst\KingKong
- %ALLUSERSPROFILE%\BaseKst\drv1028.sys

Trojan.Farfli payload sẽ thực thi như sau:

rundll32.exe rundll32 "%ALLUSERSPROFILE%\BaseKst\KingKong.dll", Install.

Tiếp theo Trojan.Farfli sẽ ghi vào registry để có thể chạy như một dịch vụ nền:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MediaControl\Parameters\"serviceDll"
- "%SYSTEMROOT%\Documents and Settings\All Users\BaseKst\KingKong.dll"

Sau đó, Trojan.Farfli sẽ kết nối tới máy chủ C&C trước khi thực thi hành động và gửi các thông tin đánh cắp được đến máy chủ C&C, với các thao tác: Mở một cửa sổ lệnh điều khiển từ xa; Ghi lại thao tác bấm phím; Đánh cắp thông tin về máy tính và mạng; Chụp ảnh màn hình.