Phòng Văn hóa và Thông tin
Huyện Đak Đoa, Tỉnh Gia Lai
12.11.2019 16:18:05 +07:00

ỦY BAN NHÂN DÂN **HUYỆN ĐAK ĐOA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1898/UBND-CNTT V/v rà quét, xử lý, bóc gỡ mã độc chiến dịch tấn công mạng có chủ đích	*Đak Đoa, ngày 12 tháng 11 năm 2019*

Kính gửi:

- Văn phòng Huyện ủy;
- Văn phòng HĐND -UBND huyện;
- Các cơ quan, đơn vị thuộc huyện;
- Các Hội, Đoàn thể huyện;
- Ủy ban nhân dân các xã, thị trấn;

Thực hiện văn bản số 1395/STTTT-CNTT ngày 31/10/2019 của Sở thông tin và Truyền thông về việc rà quét, xử lý, bóc gỡ mã độc chiến dịch tấn công mạng có chủ đích.

Ủy ban nhân dân huyện đề nghị các cơ quan, đơn vị, địa phương thực hiện gấp các biện pháp cụ thể như sau:

1. Tải công cụ rà quét, diệt các mã độc của chiến dịch APT theo đường dẫn: http://remove-apt.vnpt.vn/download/tools/incident-response-v1.0.exe;

2. Giám sát nghiêm ngặt, ngăn chặn kết nối đến các máy chủ điều khiển mã độc APT theo danh sách trong phụ lục Công văn số 1024/ CATTT-VNCERT ngày 30/10/2019 của Cục An toàn thông tin được gửi kèm;

3. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) về Ủy ban nhân dân huyện (qua Phòng Văn hóa và Thông tin) trước ngày 12 tháng 11 năm 2019 để tổng hợp, báo cáo Sở thông tin và Truyền thông.

Trên đây là loại mã độc nguy hiểm, tin tặc có thể đánh cắp thông tin, tấn công mạng leo thang đặc quyền gây ra nhiều hậu quả nghiêm trọng, Ủy ban nhân dân huyện thông báo để các cơ quan, đơn vị, địa phương biết và thực hiện./.

Nơi nhận: - Chủ tịch, các PCT UBND huyện; - Lãnh đạo Văn phòng; - Phòng Văn hóa và thông tin; - Như trên. - Lưu VT-CNTT.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** KT PHÓ CHỦ TỊCH Hoàng Nhưn

Ủy ban Nhân dân huyện Đak Đoa
Tỉnh Gia Lai
12.11.2019 15:19:28 +07:00

Ký bởi: Cục An toàn thông tin
Cơ quan: Bộ Thông tin và Truyền thông
Thời gian ký: 30/10/2019 11:22:47

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1024/CATTT-VNCERT
V/v rà quét, xử lý, bóc gỡ mã độc chiến dịch tấn công mạng có chủ đích

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

Hà Nội, ngày 30 tháng 10 năm 2019

Kính gửi:
- Các đơn vị chuyên trách về CNTT, ATTT của Văn phòng Trung ương Đảng, các Ban của Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT, ATTT các Bộ, ngành;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông;
- Các Sở thông tin và Truyền thông;
- Các Tổng công ty, Tập đoàn Kinh tế, các Tổ chức Tài chính, Ngân hàng;
- Các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông Vận tải;
- Thành viên mạng lưới ứng cứu sự cố Quốc gia.

Căn cứ Chỉ thị 14/CT-TTg của Thủ tướng Chính phủ về "nâng cao năng lực phòng, chống phần mềm độc hại", Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Thực hiện công tác theo dõi và giám sát trên không gian mạng Việt Nam, Cục An toàn thông tin đã phát hiện và ghi nhận chiến dịch tấn công mạng có tổ chức và có chủ đích (APT) với máy chủ điều khiển đặt bên ngoài lãnh thổ đã phát tán mã độc quy mô lớn nhằm vào các hệ thống thông tin của các cơ quan Chính phủ và chủ quản hệ thống thông tin hạ tầng quan trọng quốc gia tại Việt Nam. Hiện nay Cục An toàn thông tin đã xác định được hơn 400,000 địa chỉ IP bị lây nhiễm với hơn 16 biến thể của mã độc trong chiến dịch này.

Cục An toàn thông tin đề nghị các cơ quan, tổ chức, doanh nghiệp thực hiện gấp các biện pháp cụ thể như sau:

1. Hướng dẫn người sử dụng, khách hàng tải công cụ rà quét, diệt các mã độc của chiến dịch APT theo đường dẫn: http://remove-apt.vnpt.vn/download/tools/incident-response-v1.0.exe;

2. Giám sát nghiêm ngặt, ngăn chặn kết nối đến các máy chủ điều khiển mã độc APT theo danh sách trong phụ lục gửi kèm;

3. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) về Cục An toàn thông tin trước ngày 05 tháng 11 năm 2019.

Trên đây là loại mã độc nguy hiểm. Tin tặc có thể đánh cắp thông tin, tấn công mạng leo thang đặc quyền gây ra nhiều hậu quả nghiêm trọng, Cục An toàn thông tin yêu cầu Lãnh đạo các cơ quan, tổ chức, doanh nghiệp nghiêm túc thực hiện Lệnh điều phối.

Cơ quan Điều phối Quốc gia:

Cục An toàn thông tin

Địa chỉ: Tầng 5 - Tòa nhà 115 Trần Duy Hưng - Cầu Giấy - Hà Nội;

Điện thoại: 091 8228754;

Hòm thư điện tử tiếp nhận báo cáo: ir@vncert.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục trưởng (để b/c);
- Các PCT (để p/h);
- VNCERT/CC, NCSC, CNĐN, CNHCM (để t/h);
- Lưu: VT..

KT.CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

PHỤ LỤC THÔNG TIN VỀ DOMAIN VÀ IP C&C SERVER LIÊN QUAN ĐẾN MÃ ĐỘC APT

(kèm theo công văn số 1024/CATTT-VNCERT ngày 30/10/2019)

I. Danh sách các tên miền/IP máy chủ điều khiển mã độc (C&C Server)

STT	C&C	STT	C&C
1	adobephotostage.com	28	207.148.12.47
2	olk4.com	29	149.28.74.41
3	apple-net.com	30	207.148.78.101
4	wbemsystem.com	31	149.28.74.149
5	yahoorealtors.com	32	50.63.202.59
6	airdndvn.com	33	198.54.117.200
7	officeproduces.com	34	198.54.117.199
8	web.adobephotostage.com	35	198.54.117.197
9	Web.officeproduces.com	36	198.54.117.198
10	Up.officeproduces.com	37	162.255.119.150
11	We.officeproduces.com	38	167.88.180.148
12	Download.officeproduces.com	39	167.88.177.224
13	geocities.jp	40	167.88.180.3
14	update.olk4.com	41	45.248.87.14
15	www.cab-sec.com	42	91.195.240.117
16	167.88.178.24	43	103.224.182.250
17	43.254.217.67	44	167.88.177.224
18	154.221.24.47	45	167.88.178.24
19	144.202.54.86	46	185.239.226.19
20	50.63.202.94	47	185.239.226.19
21	50.63.202.67	48	45.77.209.52
22	50.63.202.82	49	167.88.178.118
23	184.168.221.94	50	185.239.226.61
24	184.168.221.82	51	45.77.184.12
25	184.168.221.71	52	167.88.178.118
26	50.63.202.73	53	185.239.226.61
27	45.32.50.150	54	45.77.184.12

II. Danh sách mã băm (HashMD5)

STT	Mã băm – MD5
1	165F8683681A4B136BE1F9D6EA7F00CE
2	9FF1D3AF1F39A37C0DC4CEEB18CC37DC
3	4FE276EDC21EC5F2540C2BABD81C8653
4	43067F28DC5208D4A070CF3CC92E29FB
5	11ADDA734FC67B9CFDF61396DE984559
6	08F25A641E8361495A415C763FBB9B71
7	01D74E6D9F77D5202E7218FA524226C4
8	6198D625ADA7389AAC276731CDEBB500
9	9B39E1F72CF4ACFFD45F45F08483ABF0
10	748DE2B2AA1FA23FA5996F287437AF1B
11	5F094CB3B92524FCED2731C57D305E78
12	9A180107EFB15A00E64DB3CE6394328D
13	05CF906B750EB335125695DA42F4EAFC
14	F62DFC4999D624D01E94B89946EC1036
15	CA775717D000888A7F71A5907B9C9208
16	AA115F20472E78A068C1BBF739C443BF
17	CE78EA4ED30DBDF6BEA66561636298F0
18	684EE90242C8552561EE58EE66016640
19	B9C10D6E459061CA6304BCCD7C94A471