BẢO HIỂM XÃ HỘI VIỆT NAM
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 322 /CNTT-HTA
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc, tấn công có chủ đích và cảnh báo lỗ hổng ATTT

Hà Nội, ngày 02 tháng 4 năm 2019

Kính gửi: - Văn phòng Bảo hiểm xã hội Việt Nam;
- Các đơn vị trực thuộc Bảo hiểm xã hội Việt Nam;
- Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương.
(Sau đây gọi chung là các đơn vị)

Theo thông tin từ đơn vị giám sát an ninh mạng của Việt Nam, trong thời gian qua đã ghi nhận chiến dịch phát tán mã độc tống tiền (GandCrab); chiến dịch tấn công có chủ đích (APT) của tin tặc nhằm vào các hệ thống thông tin của Việt Nam và cảnh báo lỗ hổng bảo mật hệ quản trị nội dung (Drupal). Cụ thể như sau:

1. Tấn công có chủ đích: Tin tặc thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt hệ thống bảo vệ an toàn thông tin (ATTT) của các hệ thống thông tin nhằm chiếm quyền điều khiển máy tính của người dùng, thông qua đó tấn công các máy tính nội bộ chứa thông tin quan trọng khác. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

2. Phát tán mã độc tống tiền: GandCrab 5.2 là phiên bản mới trong họ mã độc tống tiến GandCrab. GandCrab 5.2 được phát tán thông qua thư điện tử giả mạo từ Bộ Công an Việt Nam với tiêu đề "Goi trong Cong an Nhan dan Viet Nam" có đính kèm tệp documents.rar. Khi người dùng giải nén và mở tệp tin đính kèm, mã độc sẽ được kích hoạt và toàn bộ dữ liệu người dùng bị mã hóa, đồng thời sinh ra một tệp nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc bằng cách thanh toán qua đồng tiền điện tử để giải mã dữ liệu.

3. Lỗ hổng ATTT hệ quản trị nội dung: Drupal là hệ quản trị nội dung mã nguồn mở, được sử dụng khá phổ biến để xây dựng các cổng/trang thông tin điện tử, ứng dụng web (gọi chung là website) của các cơ quan đơn vị. Drupal đã công bố 7 lỗ hổng bảo mật, trong đó 2 lỗ hổng bảo mật có mức độ nguy hiểm cao cần được xử lý khẩn cấp. Số lượng website Drupal tại Việt Nam là khá nhiều, tuy nhiên các website này thường do đối tác bên ngoài xây dựng không bàn giao đầy đủ nên đơn vị quản lý website không biết rõ website được phát triển trên nền tảng Drupal dẫn đến tình trạng chủ quan, bỏ qua lỗ hổng ATTT được cảnh báo.

Mã độc và lỗ hổng ATTT rất nguy hiểm, có thể đánh cắp thông tin, mã hóa toàn bộ dữ liệu và phá hủy hệ thống thông tin. Tin tặc khai thác hoặc tấn công sẽ gây nhiều hậu quả nghiệm trọng khác.

Ngay khi nhận được thông báo từ đơn vị giám sát ninh mạng của Việt Nam và cơ quan điều phối ATTT quốc gia, Trung tâm CNTT đã chủ động thực hiện các kỹ thuật, áp dụng các chính sách (policy) thống nhất trên hệ thống các tường lửa bảo vệ (Palo Alto) tại các đơn vị để ngăn chặn các kết nối đến máy chủ điều khiển mã độc. Tuy nhiên, để bảo đảm ATTT một cách toàn diện, các đơn vị cần chủ động theo dõi, ngăn chặn từ máy tính của người dùng trong hệ thống do đơn vị quản lý. Trung tâm CNTT đề nghị các đơn vị triển khai một số nội dung công việc cụ thể như sau:

1. Thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại, cụ thể: lấy ý kiến của BHXH Việt Nam (Trung tâm CNTT) về thông số kỹ thuật trước khi thực hiện việc mua sắm các thiết bị điện tử có kết nối internet (như camera, wireless,…); khi đưa vào sử dụng cần rà soát, kiểm tra, đánh giá về ATTT và thiết lập cấu hình phù hợp với quy định (tuyệt đối không sử dụng cấu hình mặc định).

2. Thực hiện cài đặt phần mềm diệt virus của Ngành trang bị cho toàn bộ các thiết bị máy tính (bao gồm cả máy chủ quản trị và máy trạm) và cập nhật

theo các thông tin nhận dạng tại Phụ lục đính kèm để ngăn chặn kết nối đến các máy chủ điều khiển mã độc. Theo dõi các kết nối đến máy chủ điều khiển mã độc trên thiết bị tường lửa Palo Alto. Nếu phát hiện sự cố cần nhanh chóng cô lập máy tính đã phát hiện để xử lý.

3. Thông báo đến toàn thể công chức, viên chức và người lao động tại đơn vị nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong thư điện tử có chứa các tập tin dạng: .doc, .pdf, .zip, .rar,… được gửi từ người lạ hoặc nếu thư điện tử được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường.

4. Phối hợp với đơn vị xây dựng website rà soát nền tảng phát triển website của đơn vị, thực hiện bàn giao đầy đủ thông tin của website. Nếu website phát triển trên nền tảng Drupal cần khẩn trương cập nhật bản vá lỗ hổng ATTT cho hệ quản trị nội dung Drupal.

Trong quá trình triển khai nếu có khó khăn, vướng mắc liên hệ Trung tâm CNTT (Phòng Quản lý Hạ tầng và An ninh thông tin, điện thoại: 0243.7753102, thư điện tử: hta.cntt@vss.gov.vn) để được hỗ trợ, xử lý.

Trân trọng./.

Nơi nhận:
- Như trên;
- Tổng Giám đốc (để b/c);
- PTGĐ Phạm Lương Sơn (để b/c);
- Giám đốc (để b/c);
- Lưu: VT, HTA.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BẢO HIỂM XÃ HỘI VIỆT NAM
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Lê Vũ Toàn

PHỤ LỤC
THÔNG TIN VỀ MÁY CHỦ ĐIỀU KHIỂN MÃ ĐỘC

1. Danh sách các máy chủ điều khiển mã độc

STT	Tên miền và địa chỉ IP C&C	STT	Tên miền và địa chỉ IP C&C
1	192.227.248.189	28	107.175.75.115
2	usfinance.club	29	zzivet37.pro
3	ukfinance.online	30	wvideo.site
4	107.174.39.144	31	usfinance.store
5	184.164.139.212	32	107.175.64.217
6	shengu.tech	33	pixeliph.com
7	kalya.website	34	198.46.209.171
8	smtp3.info	35	108.170.60.181
9	urlmon.online	36	62.255.119.211
10	107.175.94.16	37	192.95.14.128
11	zivet37.services	38	kair.xyz
12	gpcantgua.com	39	autoif.online
13	107.172.3.16	40	crossfr.site
14	107.175.75.116	41	dochelp.space
15	167.114.56.226	42	185.136.165.202
16	66.85.157.69	43	107.172.249.122
17	107.172.249.103	44	198.23.140.75
18	198.46.168.33	45	107.172.150.141
19	172.245.205.107	46	185.136.163.167
20	167.114.56.224	47	151.106.60.15

21	116.197.235.202	48	198.46.168.29
22	72.83.72.137	49	151.106.60.136
23	vanxuangroup.edu.vn	50	192.227.248.181
24	gpcantgua.com	51	192.64.119.87
25	192.64.119.21	52	192.64.119.86
26	192.64.119.20	53	www.kakaocorp.link
27	192.227.248.188	54	107.173.49.208

2. Danh sách mã băm

- hs.exe MD5: df934e2d23507a7f413580eae11bb7dc
- hs.exe SHA-1:5ce51e3882c40961caf2317a3209831ed77c9c40
- HSMBalance.exe MD5: 34404a3fb9804977c6ab86cb991fb130
- HSMBalance.exe SHA-1: b345e6fae155bfaf79c67b38cf488bb17d5be56d
- ICAS.ps1 MD5: b12325a1e6379b213d35def383da2986
- ICAS.ps1 SHA-1: c48ff39e5efc6ca60c31200344c47b5de3b3605d
- MD5: 7c651d115109fd8f35fddfc44fd24518
- MD5: 8a41520c89dce75a345ab20ee352fef0
- MD5: b88d4d72fdabfc040ac7fb768bf72dcd
- MD5: E00499E21F9DCF77FC990400B8B3C2B5
- MD5: 53F7BE945D5755BB628DEECB71CDCBF2
- MD5: 9c35e9aa9255aa2214d704668b039ef6
- MD5: 25376ea6ea0903084c45bf9c57bd6e4f
- MD5: 1e2795f69e07e430d9e5641d3c07f41e
- MD5: 3be75036010f1f2102b6ce09a9299bca
- MD5: fee0b31cc956f083221cb6e80735fcc5
- MD5: 4c400910031ee3f12d9958d749fa54d5
- MD5: 2e0d13266b45024153396f002e882f15
- MD5: 26f09267d0ec0d339e70561a610fb1fd
- MD5: 09e4f724e73fccc1f659b8a46bfa7184

- MD5: 18c2adfc214c5b20baf483d09c1e1824
- MD5: 2cd8e5d871f5d6c1a8d88b1fb7372eb0
- MD5: e9130a2551dd030e3c0d7bb48544aaea
- MD5: 9888d1109d6d52e971a3a3177773efaa
- MD5: be021d903653aa4b2d4b99f3dbc986f0
- MD5: 2036a9e008d16e8ac35614946034b1a5
- MD5: ef5741c4b96ef9498357dc4d33498163
- MD5: 5B7244C47104F169B0840440CDEDE788
- MD5: cc29adb5b78300b0f17e566ad461b2c7
- MD5: DDCA6B2B2623904A072A5AF0A9E26267
-SHA1: E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74