UBND TỈNH QUẢNG TRỊ **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 110/STTTT-CNTT	*Quảng Trị, ngày 12 tháng 02 năm 2019*
V/v Theo dõi, ngăn chặn kết nối và bóc gỡ các tập tin mã độc tấn công có chủ đích vào các hệ thống thông tin	

Kính gửi:

- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

Qua theo dõi và giám sát trên không gian mạng Việt Nam trong thời gian trước và sau Tết nguyên đán Kỷ Hợi, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã ghi nhận chiến dịch tấn công có chủ đích (APT) của tin tặc nhằm vào các hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thông tin hạ tầng quan trọng quốc gia tại Việt Nam. Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và 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 của ngân hàng và tổ chức chủ quản hệ thống thông tin hạ tầng quan trọng quốc gia nhằm chiếm quyền điều khiển máy tính của người dùng; thông qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin quan trọng khác. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thông tin hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thông tin hạ tầng quan trọng quốc gia sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

Thực hiện Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ về việc ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng toàn quốc. Để bảo đảm an toàn thông tin mạng, phòng ngừa sự cố mất an toàn thông tin có thể xảy ra, Sở Thông tin và Truyền thông đề nghị thủ trưởng các cơ quan khẩn trương chỉ đạo cán bộ chuyên trách hoặc phụ trách công nghệ thông tin của cơ quan, đơn vị mình thực hiện các biện pháp sau:

1. Chủ động rà soát các điểm yếu, lỗ hổng trên hệ thống thông tin, tăng cường triển khai các biện pháp quản lý và kỹ thuật nhằm bảo đảm an toàn thông tin cho hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, đơn vị và các hệ thống cung cấp dịch vụ công phục vụ người dân, doanh nghiệp.

2. Theo dõi và ngăn chặn kết nối đến các máy chủ C&C có tên miền và địa chỉ IP sau:

STT	C&C	STT	C&C
1	192.227.248.189	27	192.227.248.188
2	usfinance.club	28	107.175.75.115
3	ukfinance.online	29	zzivet37.pro
4	107.174.39.144	30	wvideo.site
5	184.164.139.212	31	usfinance.store
6	shengu.tech	32	107.175.64.217
7	kalya.website	33	pixeliph.com
8	smtp3.info	34	198.46.209.171
9	urlmon.online	35	108.170.60.181
10	107.175.94.16	36	62.255.119.211
11	zivet37.services	37	192.95.14.128
12	gpcantgua.com	38	kair.xyz
13	107.172.3.16	39	autoif.online
14	107.175.75.116	40	crossfr.site
15	167.114.56.226	41	dochelp.space
16	66.85.157.69	42	185.136.165.202
17	107.172.249.103	43	107.172.249.122
18	198.46.168.33	44	198.23.140.75

STT	C&C	STT	C&C
19	172.245.205.107	45	107.172.150.141
20	167.114.56.224	46	185.136.163.167
21	116.197.235.202	47	151.106.60.15
22	72.83.72.137	48	198.46.168.29
23	vanxuangroup.edu.vn	49	151.106.60.136
24	gpcantgua.com	50	192.227.248.181
25	192.64.119.21	51	192.64.119.87
26	192.64.119.20	52	192.64.119.86

3. Rà quét hệ thống, xoá các thư mục và bóc gỡ tập tin mã độc có dấu hiệu tương ứng sau:

- MD5: 25376ea6ea0903084c45bf9c57bd6e4f
- MD5: 1e2795f69e07e430d9e5641d3c07f41e
- MD5: 3be75036010f1f2102b6ce09a9299bca
- HSMBalance.exe MD5: 34404a3fb9804977c6ab86cb991fb130
- HSMBalance.exe SHA-1:b345e6fae155bfaf79c67b38cf488bb17d5be56d
- ICAS.ps1 MD5: b12325a1e6379b213d35def383da2986
- ICAS.ps1 SHA-1: c48ff39e5efc6ca60c31200344c47b5de3b3605d
- MD5: 7c651d115109fd8f35fdfc44fd24518
- MD5: 8a41520c89dce75a345ab20ee352fef0
- MD5: b88d4d72fdabfc040ac7fb768bf72dcd
- hs.exe MD5: df934e2d23507a7f413580eae11bb7dc
- hs.exe SHA-1:5ce51e3882c40961caf2317a3209831ed77c9c40
- 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: 53F7BE945D5755BB628EECB71CDCBF2
- MD5: E00499E21F9DC990400B8B3C2B5
- MD5: 9c35e9aa9255a2214d704668b039ef6
- MD5: cc29adb5b78300b0f17e566ad461b2c7
- MD5: C6774C1417BE2E8B7D14BAD1391|1DO4B

Trên đây là những mã độc rất nguy hiểm, có thể đánh cắp thông tin và phá hủy hệ thống thông tin các cơ quan nhà nước; Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị quan tâm thực hiện.

Mọi thông tin xin liên hệ: Sở Thông tin và Truyền thông - Thành viên mạng lưới Ứng cứu sự cố mạng Internet Việt Nam do Bộ Thông tin và Truyền thông thành lập. Đơn vị thường trực kỹ thuật: Trung tâm Công nghệ thông tin và Truyền thông, điện thoại 0233. 3504909.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (*báo cáo*);
- Trung tâm CNTT-TT (*phối hợp thực hiện*);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG TRỊ

Người ký: Nguyễn Thị Huyền
Email: nguyenthihuyenqt@quangtri.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Quảng Trị
Chức vụ: Phó Giám đốc
Thời gian ký: 12.02.2019 15:23:32 +07:00

Nguyễn Thị Huyền