UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số:670 /STTTT-BCVTCNTT

Hà Nam, ngày 10 tháng 7 năm 2020

V/v cảnh báo lỗ hổng trên hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng trên thiết bị F5 BIG-IP và tình hình an toàn thông tin trên địa bàn tỉnh

Kính gửi:
- Các sở, ban, ngành, đoàn thể thuộc tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Hà Nam, Trường Chính trị tỉnh.

Căn cứ Báo cáo số 20/BC-CATT ngày 02/7/2020 của Cục An toàn thông tin về việc báo cáo kỹ thuật tình hình an toàn thông tin tháng 6/2020 và thống kê kết nối chia sẻ của các tỉnh/thành;

Thực hiện Công văn số 564/CATTT-NCSC ngày 07/7/2020 của Cục An toàn thông tin về việc nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức sử dụng thiết bị F5 BIG-IP;

Để nâng cao năng lực phòng, chống phần mềm độc hại và kịp thời vá các lỗ hổng bảo mật, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị:

1. Thực hiện theo hướng dẫn của Cục An toàn thông tin tại Công văn số 564/CATTT-NCSC (*Có bản sao Công văn gửi kèm theo*).

2. Trang bị phần mềm diệt virus có bản quyền cho toàn bộ máy tính của cơ quan để thực hiện quét mã độc (hiện nay trên địa bàn tỉnh đang tồn tại các dạng mã độc Avalanche, Conficker, Sality…).

3. Thực hiện kiểm tra và xử lý ngay các lỗ hổng bảo mật nguy hiểm còn tồn tại trên các máy tính chưa được xử lý và khắc phục (*Mục 1, Phụ lục*).

4. Thực hiện rà soát để phát hiện và xử lý các lỗ hổng phổ biến trên các máy tính (*Mục 2, Phụ lục*)

5. Phổ biến cho các cán bộ, công chức, viên chức thông tin về các loại mã độc/botnet để biết và phòng tránh lây nhiễm cho các máy tính (*Mục 3, Phụ lục*).

Khi phát hiện có dấu hiệu mất an toàn thông tin tại cơ quan, đơn vị và xử lý các lỗi bảo mật nếu có vướng mắc đề nghị liên hệ:

- Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam). Điện thoại: **0226.3846333**, thư điện tử: **ttcntt@hanam.gov.vn**.

- Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại **0243.209.1616**, thư điện tử: **ais@mic.gov.vn**.

Nơi nhận:
- Như trên;
- UBND tỉnh (để b/c)
- Lưu VT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HÀ NAM

Nguyễn Đức Cường

Phụ lục

Danh sách và thông tin các lỗ hổng gây mất an toàn thông tin

(Kèm theo Công văn số: /STTTT-BCVTCNTT ngày /7/2020 của Sở Thông tin và Truyền thông)

1. Các lỗ hổng còn tồn tại trên nhiều máy tính, chưa được xử lý, khắc phục

STT	Tên lỗ hổng	Mô tả tóm tắt
1	CVE-2019-0708	Lỗ hổng trong dịch vụ Remote Desktop của hệ điều hành Windows
2	CVE-2013-3900(MS13-098)	Lỗ hổng trong hệ điều hành Windows
3	CVE-2015-0009(MS15-014)	Lỗ hổng trong Group Policy của Microsoft Windows cho phép đối tượng tấn công truy cập trái phép.

2. Danh sách điểm yếu lỗ hổng phổ biến đã có bản cập nhật

STT	Mã điểm yếu/ lỗ hổng
1	CVE-2019-0708
2	CVE-2013-3900 (MS13-098)
3	CVE-2014-4114(MS14-060)
4	CVE-2015-0009(MS15-014)
5	CVE-2015-1635(MS15-034)
6	CVE-2015-0084(MS15-028)
7	CVE-2014-0315(MS14-019)
8	CVE-2017-0144(MS17-010)
9	CVE-2013-3129 (MS13-053)
10	CVE-2015-0073(MS15-025)
11	CVE-2015-0080(MS15-024)
12	CVE-2015-0076(MS15-029)
13	CVE-2013-3940(MS13-089)
14	CVE-2015-0012(MS15-017)

STT	Mã điểm yếu/ lỗ hổng
15	CVE-2014-0260(MS14-001)
16	CVE-2014-1818(MS14-036)
17	CVE-2014-6352(MS14-064)
18	CVE -2014-0263(MS14-007)
19	CVE-2014-4148(MS14-058)
20	CVE-2015-0078(MS15-023)
21	CVE-2008-4250 (MS08-067)
22	CVE-2014-2778 (MS14-034)
23	CVE-2013-3891 (MS13-086)

3. Thông tin về các loại mã độc/botnet

Tên gọi	Một số IP - Tên miền	Mô tả
Avalanche (Win32/Gamarue)	somicrososoft.ru morphed.ru a.deltaheavy.ru hzmksreiuojy.in devicesta.ru designthefuture.ru andall.anddddzandddd2.com ochengorit.ru and32.microscobisoftng5.com letstryitnowx.online cp.4jhlti79.ru cp.oa505txz.ru cp.qc0zt6eo.ru cp.4nbizac8.ru b.deltaheavy.ru c.deltaheavy.ru cp.x1yuqjh9.ru and19.themarket12345sushi3.com cp.ekic4bf5.ru	- Thời gian xuất hiện: Năm 2011. - Mục tiêu tấn công: Doanh nghiệp sử dụng thẻ thanh toán. - Các chức năng chính như: Keylogging; Rootkit; Truy cập từ xa ẩn; Thu thập thông tin đăng nhập từ trình duyệt. - Mục đích chính là phát tán các dòng mã độc khác nhằm phục vụ các cuộc tấn công phần mềm độc hại toàn cầu. Mạng botnet Andromeda bao gồm và có liên quan đến ít nhất 80 họ phần mềm độc hại, trong đó chủ yếu là họ mã độc Point of Sale (POS), ví dụ như GamaPOS.

Tên gọi	Một số IP - Tên miền	Mô tả
SmokeLoader	173.231.184.57 173.231.184.5 206.189.61.126 ukcompany.me ukcompany.pw ukcompany.top	-Thời gian xuất hiện: Năm 2011 và đã từng tham gia trong các chiến dịch email giả mạo, với tần suất không thường xuyên nhưng vẫn tiếp tục được phát triển. Xuất hiện từ đầu tháng 01/2018, Meltdown và Specter là hai phương pháp tấn công qua kênh mới nhắm vào bộ vi xử lý hiện đại và được cho là ảnh hưởng đến hàng tỷ thiết bị. Đây là các lỗ hổng ở cấp CPU, cho phép các ứng dụng độc hại truy cập vào dữ liệu khi đang được xử lý, bao gồm mật khẩu, ảnh, tài liệu, email và những thứ tương tự. Mã độc Smoke Loader đặc biệt hoạt động mạnh trong suốt năm 2018 với nhiều chiến dịch phát tán Smoke Loader qua các bản vá lỗi giả mạo dành cho lỗ hổng Meltdown và Spectre.
Conficker	149.93.100.83 149.93.123.143 149.93.131.229 149.93.132.110 149.93.138.146 149.93.149.250 149.93.154.218 149.93.155.237 149.93.16.132	- Thời gian phát hiện: từ tháng 10/2008. - Lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật. - Mục tiêu: Nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác

Tên gọi	Một số IP - Tên miền	Mô tả
	149.93.16.142 149.93.170.119 149.93.173.38 149.93.179.14 149.93.179.249 149.93.180.45 149.93.184.113 149.93.196.247 149.93.2.46 149.93.20.179 149.93.203.187	
Sality (KuKu)	4b998.bmakemegood24.com axr.lukki6nd2kdnc.info bdd.f5ds1jkkk4d.info blog.inform1ongung.info businecessity.com dddrbcash.net dyfa.lukki6nd2kdnc.info gyi.f5ds1jkkk4d.info jcnqg.lukki6nd2kdnc.info	- Thời gian phát hiện: lần đầu tiên bị phát hiện vào 04/6/2003. - Tấn công vào các máy tính sử dụng hệ điều hành Windows, - Thời điểm Sality là một mã độc lây nhiễm vào hệ thống qua các đoạn mã chèn vào đầu tập tin host để mở cửa hậu và lấy trộm thông tin bàn phím. Đến năm 2010 xuất hiện biến thể Sality nguy hiểm hơn và trở thành một trong những dòng mã độc phức tạp và nguy hiểm nhất đối với an toàn của hệ thống. Máy tính bị nhiễm mã độc sẽ trở thành một điểm trong mạng ngang hàng để tiếp tục phát tán mã độc sang

Tên gọi	Một số IP - Tên miền	Mô tả
	jlw.lukki6nd2kdnc.info jwyo.f5ds1jkkk4d.info kukutrustnet666.info mdagk.f5ds1jkkk4d.info mim.lukki6nd2kdnc.info opxp.f5ds1jkkk4d.info qdxc.lukki6nd2kdnc.info rqkh.f5ds1jkkk4d.info rvj.lukki6nd2kdnc.info trfqi.f5ds1jkkk4d.info vawp.lukki6nd2kdnc.info	các máy tính khác. Sality chủ yếu để phát tán thư rác, tạo ra các proxy, ăn cắp thông tin cá nhân, lây nhiễm vào các máy chủ web để biến các máy chủ này thành máy chủ điều khiển của mạng botnet để tiếp tục mở rộng mạng botnet.