VIỆN HÀN LÂM
KHOA HỌC VÀ CÔNG NGHỆ VN
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Số: 145 /THTT

V/v thông báo tình hình an toàn không gian mạng tháng 3

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

Hà Nội, ngày 11 tháng 5 năm 2021

Kính gửi: Các đơn vị trực thuộc

Thực hiện chỉ đạo của PGS. TS. Trần Tuấn Anh, Phó Chủ tịch Viện Hàn lâm Khoa học và Công nghệ Việt Nam giao Trung tâm Tin học và Tính toán rà soát tình hình an toàn không gian mạng của Viện Hàn lâm được nêu ra trong Báo cáo số 10/BC-CATTT ngày 08/04/2021 của Cục An toàn Thông tin – Bộ Thông tin và Truyền thông, Trung tâm Tin học và Tính toán đã rà soát, thống kê về thực trạng lây nhiễm virus/mã độc trên các máy tính cá nhân tại các đơn vị trực thuộc Viện Hàn lâm, cụ thể là:

- Có 8 đơn vị trực thuộc với tổng số 11 máy tính bị nhiễm mã độc Avalanche và Wannacry.

- Có 16 đơn vị trực thuộc với tổng số 84 máy tính bị nhiễm virus các loại.

Trung tâm Tin học và Tính toán thông báo đến các đơn vị được biết để rà soát gỡ bỏ virus/mã độc trên máy tính cá nhân thuộc đơn vị quản lý.

(Danh sách các đơn vị có máy tính bị nhiễm virus/mã độc trong phần phụ lục kèm theo hướng dẫn xử lý).

Trong trường hợp cần hỗ trợ kỹ thuật, xin vui lòng liên hệ với đồng chí Trần Văn Sinh, Phòng Đảm bảo công nghệ thông tin – Trung tâm Tin học và Tính toán qua số điện thoại 024.37914773; thư điện tử: sinhtv@cic.vast.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Viện Hàn lâm KHCNVN (để b/c);
- Giám đốc (để b/c);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Ngô Văn Thanh

PHỤ LỤC

(Kèm theo Công văn số /THTT ngày tháng 5 năm 2021
của Trung tâm Tin học và Tính toán)

a) Danh sách các đơn vị và địa chỉ máy tính bị lây nhiễm mã độc wanacry và avalanche theo báo cáo Cục ATTT (tháng 4 năm 2021)

STT	Tên đơn vị	IP public lây nhiễm	IP nội bộ tại đơn vị	Loại mã độc nghi bị lây nhiễm	IP máy chủ Botnet
1	Vật lý địa cầu & Viện hóa học các hợp chất thiên nhiên	210.86.231.167	10.17.3.137 10.17.20.153	**Avalanche**	**184.105.192.2**
2	Viện kỹ thuật nhiệt đới	210.86.231.168	10.17.21.241	**Wannacry**	**104.17.244.81**
3	Bảo tàng thiên nhiên Việt Nam	210.86.231.172	10.17.7.187 10.17.7.5	**Avalanche**	**35.229.93.46**
4	Viện Địa chất và vật lý biển	210.86.231.173	10.17.23.189	**Avalanche**	**184.105.192.2**
5	Viện công nghệ vũ trụ và Chương trình vũ trụ	210.86.231.175	10.17.22.150	**Avalanche**	**178.162.203.202**
6	Viện sinh thái và tài nguyên sinh vật	210.86.231.178	10.17.8.136 10.17.8.126	**Avalanche**	**184.105.192.2**
7	Ban quản lý dự án USTH	123.30.9.44	10.17.40.152	**Avalanche**	**184.105.192.2**
8	Viện Địa chất và vật lý biển	210.86.231.173	10.17.23.189	**Wannacry**	**104.16.173.80**

b) Danh sách các đơn vị trực thuộc Viện Hàn lâm và địa chỉ máy tính bị lây nhiễm mã độc khác (tháng 4 năm 2021)

STT	Tên đơn vị	IP nội bộ tại đơn vị	Loại mã độc bị lây nhiễm	Ghi chú
1	Viện Kỹ thuật nhiệt đới	10.17.21.229 10.17.21.37 10.17.21.45 10.17.21.39	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web…
		10.17.21.229 10.17.21.37 10.17.21.45 10.17.21.39	MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection	Mã độc đánh cắp mật khẩu người dùng
		10.17.21.229 10.17.21.37 10.17.21.45	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
2	Viện Hóa học các hợp chất thiên nhiên	10.17.20.112 10.17.20.92	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web…
			MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection	Mã độc đánh cắp mật khẩu người dùng
		10.17.20.100 10.17.20.67 10.17.20.24	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.20.72 10.17.20.153	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.20.67	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
3	Viện Vật lý địa cầu	10.17.3.112 10.17.3.119 10.17.3.62	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web…
			MALWARE-CNC Win.Trojan.Nvbpass	Mã độc đánh cắp mật khẩu người

		10.17.3.37	variant outbound connection	dùng
		10.17.3.137	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.3.62 10.17.3.171 10.17.3.7 10.17.3.186	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.3.144	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
		10.17.3.225	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.3.144	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ liệu (Wannacry) và chiếm quyền điều khiển máy tính
4	Bảo tàng thiên nhiên	10.17.7.54	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web…
			MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection	Mã độc đánh cắp mật khẩu người dùng
		10.17.7.111	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.7.54	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.7.145 10.17.7.54	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.7.111 10.17.7.115	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo

		10.17.7.111 10.17.7.80 10.17.7.54	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ liệu (Wannacry) và chiếm quyền điều khiển máy tính
5	Học viện KHCN	10.17.35.115	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ liệu (Wannacry) và chiếm quyền điều khiển máy tính
6	Ban Quản lý dự án USTH	10.17.40.7 10.17.40.106	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web. Mã độc đánh cắp cookie, tài khoản, mật khẩu từ các trình duyệt web: Chrome, firefox, opera, …
			PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.40.138	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
7	Tầng 1 tòa nhà trung tâm	10.17.50.119	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.50.119 10.17.50.84	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
		10.17.50.24	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ liệu (Wannacry) và chiếm quyền điều khiển máy tính
8	Viện Công nghệ Vũ trụ và Chương trình	10.17.22.44	MALWARE-CNC Win.Trojan.Zegost	Là mã độc Backdoor chạy trên máy

	vũ trụ		variant outbound connection	tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.22.170	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
9	Viện Hóa học	10.17.4.123	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.4.123 10.17.4.120	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
10	Viện Sinh thái và tài nguyên sinh vật	10.17.8.36	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.8.36 10.17.8.224 10.17.8.164	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.8.166 10.17.8.227 10.17.8.183	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.8.120 10.17.8.36	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
11	Viện Địa chất và vật lý biển	10.17.23.82	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection	Lây nhiễm qua Click quảng cáo trên trang web. Mã độc đánh cắp cookie, tài khoản, mật khẩu từ các trình duyệt web: Chrome, firefox, opera, …
			MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection	Mã độc đánh cắp mật khẩu người dùng
		10.17.23.85 10.17.23.198	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.23.63	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền

				điều khiển máy tính
12	Trung tâm phát triển công nghệ cao	10.17.26.172 10.17.26.75	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.26.107 10.17.26.52	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
		10.17.26.52	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ liệu (Wannacry) và chiếm quyền điều khiển máy tính
13	Trung tâm Thông tin tư liệu	10.17.30.253	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
14	Trung tâm đào tạo và chuyển giao công nghệ	10.17.29.117	MALWARE-CNC Win.Trojan.Zegost variant outbound connection	Là mã độc Backdoor chạy trên máy tính cho phép hacker chiếm quyền điều khiển máy tính
15	Viện khoa học vật liệu	10.17.2.148 10.17.2.41	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.2.121 10.17.2.47	PUA-OTHER XMRig cryptocurrency mining pool connection attemp	Virus đào tiền ảo
		10.17.2.26	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	Loại mã độc ăn cắp thông tin tài khoản ngân hàng và ăn cắp dữ liệu người dùng
		10.17.2.23 10.17.2.148 10.17.2.20	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1). Kẻ tấn công khai thác thành công lỗ hổng sẽ thực hiện mã hóa dữ

				liệu (Wannacry) và chiếm quyền điều khiển máy tính
16	Chương trình Tây nguyên 3	10.17.43.224 10.17.43.226	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
		10.17.43.226	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo

c) Hướng dẫn xử lý virus/mã độc trên máy tính cá nhân

+ Cài phần mềm diệt virus bản quyền hoặc kích hoạt phần mềm miễn phí Defender/Windows Security có sẵn của hệ điều hành Windows 7, 8 hoặc Windows 10.

+ Sử dụng các phần mềm nêu trên rà quét toàn bộ máy tính cá nhân. Đặc biệt là những máy tính có địa chỉ IP nội bộ trong danh sách cần ưu tiên xử lý trước nhằm hạn chế lây nhiễm mã độc qua hệ thống mạg của Viện Hàn lâm.