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

Số: 269 /THTT
V/v thông báo tình hình ATTT tại Viện Hàn lâm tháng 05/2022 và hướng dẫn xử lý virus/mã độc

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

Hà Nội, ngày 20 tháng 6 năm 2022

Kính gửi: Các đơn vị trực thuộc
Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Căn cứ Báo cáo số 6/BC-CATTT ngày 07/06/2022 của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông về tình hình an toàn thông tin tháng 05/2022 và thống kê kết nối chia sẻ dữ liệu về mã độc, giám sát, Trung tâm Tin học và Tính toán thông báo như sau:

- Tại thời điểm tháng 05/2022, Viện Hàn lâm Khoa học và Công nghệ Việt Nam có 02 địa chỉ IP Public thuộc "Danh sách các đơn vị phát hiện có địa chỉ IP nằm trong mạng Botnet" của Cục An toàn thông tin.

- Trung tâm Tin học và Tính toán đã tiến hành rà quét trên hệ thống bảo mật và phát hiện virus/mã độc nguy hiểm khác nằm rải rác trong các đơn vị trực thuộc Viện Hàn lâm KHCNVN *(chi tiết tại Phụ lục kèm theo).*

Trung tâm Tin học và Tính toán kiến nghị Thủ trưởng các đơn vị chỉ đạo bộ phận chuyên trách về công nghệ thông tin tại đơn vị hoặc thuê dịch vụ để khẩn trương xử lý triệt để virus/mã độc trên các máy tính cá nhân do đơn vị quản lý *(theo địa chỉ IP được liệt kê tại Phụ lục kèm theo)*.

Trân trọng./.

Nơi nhận:
- Như trên;
- Viện Hàn lâm KHCNVN (để b/c);
- PCT. Trần Tuấn Anh (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

Phạm Hồng Công

Phụ lục

(Kèm theo Công văn số /THTT ngày /6/2022 của Trung tâm Tin học và Tính toán)

DANH SÁCH ĐƠN VỊ VÀ IP PUBLIC BỊ LÂY NHIỄM MÃ ĐỘC AVALANCHE THEO CẢNH BÁO CỦA CỤC ATTT (THÁNG 5 NĂM 2022)

STT	Tên đơn vị	IP public lây nhiễm	IP nội bộ tại đơn vị	Loại mã độc lây nhiễm	IP máy chủ Botnet
1	Viện Hóa hợp chất thiên nhiên	210.86.231.167	10.17.20.164	**Avalanche**	**173.231.184.124**
2	Viện Hóa học	210.86.231.168	10.17.4.31	**Avalanche**	**216.218.185.162**

DANH SÁCH CÁC ĐƠN VỊ TRỰC THUỘC VIỆN HÀN LÂM VÀ ĐỊA CHỈ MÁY TÍNH BỊ LÂY NHIỄM MÃ ĐỘC KHÁC (THÁNG 05 NĂM 2022)

TT	Tên đơn vị	IP nội bộ tại đơn vị	Loại mã độc bị lây nhiễm	Ghi chú
1	Viện Hóa học các hợp chất thiên nhiên	10.17.20.108 10.17.20.251 10.17.20.116	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.20.65 10.17.20.104 10.17.20.139	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
		10.17.20.164	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
2	Viện Vật lý địa cầu	10.17.3.225 10.17.3.199	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.3.90 10.17.3.172 10.17.3.177	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

TT	Tên đơn vị	IP nội bộ tại đơn vị	Loại mã độc bị lây nhiễm	Ghi chú
		10.17.3.199	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
3	Bảo tàng Thiên nhiên Việt Nam	10.17.7.46	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
		10.17.7.125 10.17.7.123 10.17.7.46	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
			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
		10.17.7.46 10.17.7.123	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
4	Viện Sinh thái và Tài nguyên sinh vật	10.17.8.116 10.17.8.248 10.17.8.237 10.17.8.3	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
		10.17.8.27 10.17.8.196	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

TT	Tên đơn vị	IP nội bộ tại đơn vị	Loại mã độc bị lây nhiễm	Ghi chú
5	Trung tâm Phát triển công nghệ cao	10.17.26.126 10.17.26.8 10.17.26.60	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
		10.17.26.131 10.17.26.18	MALWARE-CNC Win.Trojan. Zegost variant outbound connection	Virus đào tiền ảo
6	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
7	Viện Kỹ thuật nhiệt đới	10.17.21.79 10.17.21.41 10.17.21.53	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
8	Trạm y tế - Văn phòng	10.17.42.132 10.17.42.158 10.17.42.143	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
			PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
9	Viện Hóa học	10.17.4.31	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
		10.17.4.31 10.17.4.9 10.17.4.156	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
10	Trung tâm Nghiên cứu và Chuyển giao CN	10.17.29.206	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

TT	Tên đơn vị	IP nội bộ tại đơn vị	Loại mã độc bị lây nhiễm	Ghi chú
			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
11	Viện Công nghệ Vũ trụ	10.17.22.48	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	Tầng 1 Tòa nhà Trung tâm	10.17.50.108 10.17.50.177	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
			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	Tầng 7 Tòa nhà Trung tâm	10.17.58.23	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
14	Viện công nghệ thông tin	10.17.15.2	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, …

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.
- 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 mạng của Viện Hàn lâm./.