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

Số: 299 /THTT
V/v thông báo tình hình ATTT tại Viện Hàn lâm tháng 06/2023 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 28 tháng 7 năm 2023

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

Căn cứ Báo cáo số 15/BC-CATTT ngày 18/07/2023 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về tình hình an toàn thông tin tháng 06/2023 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 06/2023, Viện Hàn lâm Khoa học và Công nghệ Việt Nam có 02 IP nằm trong "Danh sách các đơn vị phát hiện có địa chỉ IP nằm trong mạng Botnet" của Cục ATTT.

- Trung tâm Tin học và Tính toán đã tiến hành rà quét trên hệ thống bảo mật của Viện Hàn lâm KHCNVN và phát hiện virus/mã độc nguy hiểm khác nằm rải rác trong các đơn vị trực thuộc Viện Hàn lâm KHCNVN.

Trung tâm Tin học và Tính toán kiến nghị Thủ trưởng các đơn vị trực thuộc Viện Hàn lâm KHCNVN chỉ đạo 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)* để không ảnh hưởng đến hệ thống mạng chung của Viện Hàn lâm KHCNVN.

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

DANH SÁCH ĐƠN VỊ TRỰC THUỘC VIỆN HÀN LÂM KHCNVN VÀ IP PUBLIC BỊ LÂY NHIỄM MÃ ĐỘC AVALANCHE THEO CẢNH BÁO CỤC ATTT (THÁNG 6 NĂM 2023)

(Kèm theo Công văn số /THTT ngày /7/2023 của Trung tâm Tin học và Tính toán)

TT	Tên đơn vị	IP public lây nhiễm	IP nội bộ tại đơn vị	Loại mã độc lây nhiễm	IP máy chủ Botnet
1	Viện Sinh thái và Tài nguyên sinh vật	210.86.230.178	10.17.8.36	*Avalanche-andromeda*	*107.6.74.81*
		210.86.230.168	10.17.8.168	*Avalanche-andromeda*	*184.105.192.2*

DANH SÁCH CÁC ĐƠN VỊ TRỰC THUỘC VIỆN HÀN LÂM KHCNVN VÀ ĐỊA CHỈ MÁY TÍNH BỊ LÂY NHIỄM MÃ ĐỘC KHÁC (THÁNG 06 NĂM 2023)

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	10.17.20.121	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
2	Viện Kỹ thuật nhiệt đới	10.17.21.225	PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
			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
			PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
3	Viện Địa chất và Địa vật lý biển	10.17.23.28 10.17.23.104 10.17.23.160	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
4	Trung tâm Nghiên cứu và Phát triển công nghệ cao	10.17.26.165	PUA-OTHER XMRig cryptocurrency mining pool connection attempt	Virus đào tiền ảo
			PUA-OTHER Cryptocurrency Miner outbound connection attempt	Virus đào tiền ảo
5	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
6	Trạm Y tế (thuộc Văn phòng Viện Hàn lâm KHCNVN)	10.17.42.39 10.17.42.142 10.17.42.190	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

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 từ Windows 7 trở lên.

- 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 KHCNVN./.