BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM **Độc lập - Tự do - Hạnh phúc**
Số: 2290/BTTTT - CATTT V/v hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật	*Hà Nội, ngày 11 tháng 7 năm 2018*

Kính gửi:

- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Cơ quan Trung ương của các đoàn thể;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các tập đoàn kinh tế, tổng công ty Nhà nước.

Căn cứ Luật An toàn thông tin mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Ngày 25/5/2018, Thủ tướng Chính phủ có Chỉ thị số 14/CT-TTg về việc nâng cao năng lực phòng, chống phần mềm độc hại, trong đó nêu rõ:

Các bộ, cơ quan, ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới.

Giải pháp phòng, chống mã độc được đầu tư mới hoặc nâng cấp cần có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích, gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật.

Trên cơ sở đó, Bộ Thông tin và Truyền thông ban hành hướng dẫn kết nối, trao đổi, chia sẻ thông tin, dữ liệu về mã độc giữa các hệ thống kỹ thuật của cơ

quan chức năng liên quan với giải pháp phòng, chống mã độc ở các bộ, ngành, địa phương, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật *(kèm theo)*.

Bản mềm tài liệu hướng dẫn có thể tải về từ Cổng thông tin điện tử của Bộ tại địa chỉ: http://mic.gov.vn hoặc của Cục An toàn thông tin: https://ais.gov.vn

Việc kết nối, trao đổi, chia sẻ thông tin dữ liệu về mã độc để phục vụ theo dõi, tổng hợp, đánh giá chỉ số lây nhiễm phần mềm độc hại ở các bộ, ngành, địa phương, coi đây là một trong những tiêu chí đánh giá mức độ bảo đảm an toàn thông tin của các bộ, ngành, địa phương.

Bộ Thông tin và Truyền thông định kỳ hàng quý tổng hợp tình hình báo cáo Thủ tướng Chính phủ.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, đề nghị quý cơ quan phản hồi, góp ý để Bộ Thông tin và Truyền thông nghiên cứu, xem xét cập nhật hướng dẫn cho phù hợp với tình hình triển khai thực tế trong từng giai đoạn cụ thể.

Chi tiết xin liên hệ: Ông Nguyễn Huy Dũng, Phó Cục trưởng Cục An toàn thông tin, Bộ Thông tin và Truyền thông, thư điện tử: nhdung@mic.gov.vn, điện thoại: 0916786018.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ (qua thư điện tử);
- Đơn vị chuyên trách về CNTT của Văn phòng TƯ Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Đơn vị chuyên trách về CNTT của Cơ quan Trung ương của các đoàn thể;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương (qua thư điện tử);
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Hưng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

HƯỚNG DẪN
KẾT NỐI, CHIA SẺ THÔNG TIN VỀ MÃ ĐỘC GIỮA CÁC HỆ THỐNG KỸ THUẬT

(Ban hành kèm theo công văn số 2290 /BTTTT-CATTT ngày 17/7/2018)

1. Phạm vi và đối tượng áp dụng

1.1. Phạm vi áp dụng

Tài liệu này nhằm hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật trong các cơ quan, tổ chức nhà nước.

1.2. Đối tượng áp dụng

Đối tượng áp dụng bao gồm:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

- Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Toà án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán Nhà nước, Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam, Tổng Liên đoàn Lao động Việt Nam, Trung ương Đoàn Thanh niên cộng sản Hồ Chí Minh, Trung ương Hội Liên hiệp Phụ nữ Việt Nam, Hội Cựu chiến binh Việt Nam, Hội Nông dân Việt Nam có thể tham khảo và áp dụng trong cơ quan, tổ chức mình.

- Các cơ quan, tổ chức, doanh nghiệp khác có thể tham khảo và áp dụng trong cơ quan, tổ chức mình.

2. Áp dụng tiêu chuẩn, quy chuẩn kỹ thuật

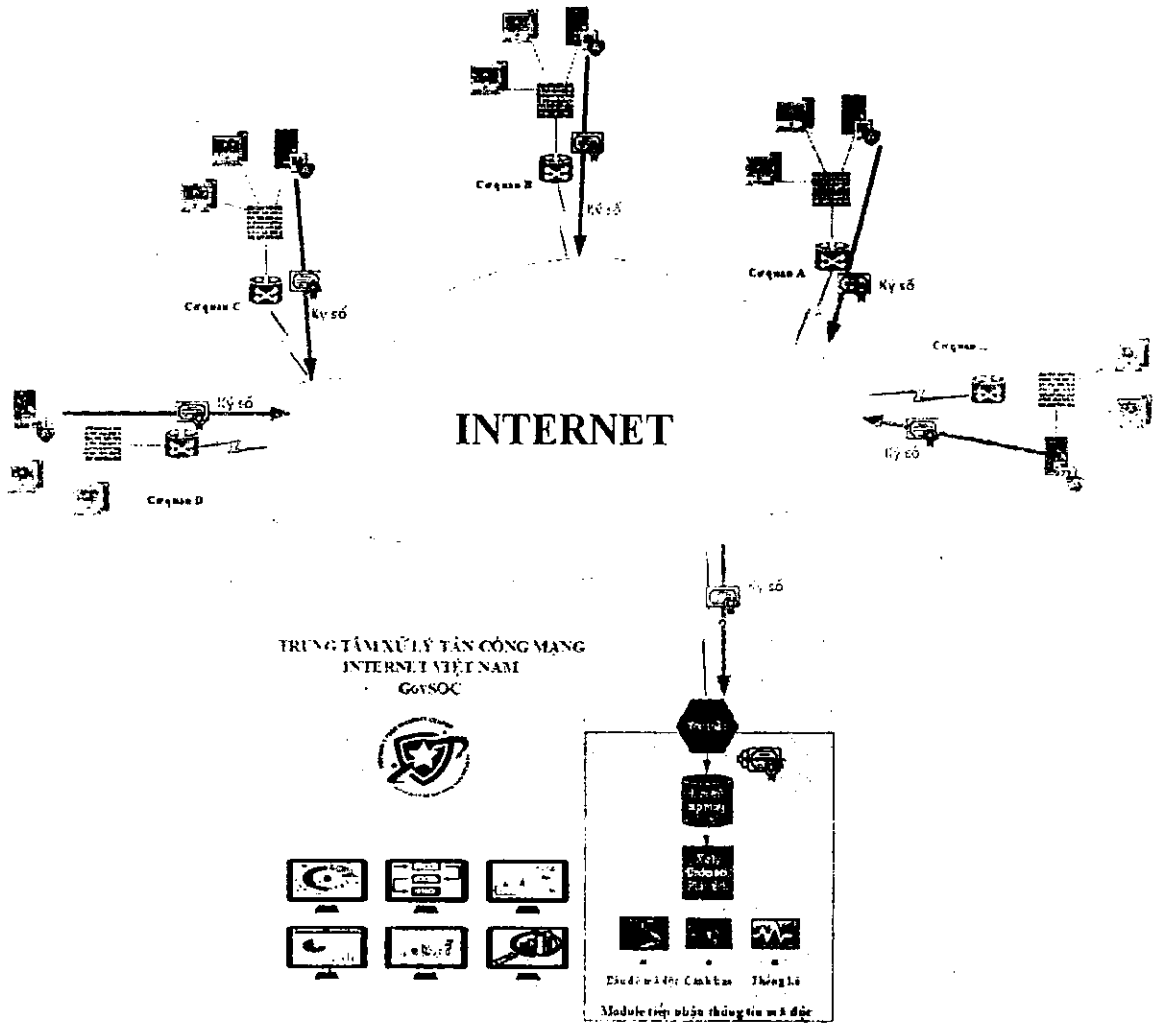
Việc kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật trong các cơ quan, tổ chức nhà nước tuân thủ theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước; Thông tư số 13/2017/TT-BTTTT Quy định các yêu cầu kỹ thuật về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia.

Tham chiếu áp dụng Quy chuẩn kỹ thuật quốc gia QCVN 102:2016/BTTTT về cấu trúc mã định danh và định dạng dữ liệu gói tin phục vụ

kết nối các hệ thống quản lý văn bản và điều hành đối với việc áp dụng định dạng gói tin edXML (hướng dẫn cụ thể bên dưới) và mã định danh của các cơ quan, tổ chức.

3. Mô hình và phương thức kết nối

3.1. Mô hình kết nối



Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có giải pháp phòng, chống mã độc được đầu tư mới hoặc nâng cấp cần có chức năng cho phép quản trị tập trung, có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông (Cục An toàn thông tin).

Do vậy mỗi cơ quan tổ chức khi triển khai các giải pháp phòng, chống mã độc cần có máy chủ quản lý tập trung về tình hình lây nhiễm, phòng chống mã

độc của các máy tính, thiết bị mạng trong nội bộ cơ quan, tổ chức và chia sẻ thông tin cơ bản với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông.

Việc kết nối, chia sẻ thông tin về mã độc giúp cập nhật tình hình lây nhiễm mã độc chung tại Việt Nam. Các cơ quan tổ chức gửi thông tin về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) có thể cập nhật tình hình của tổ chức mình và tổ chức khác thông qua bản đồ lây nhiễm mã độc tại Việt Nam.

Với các mẫu, thông tin mã độc thu thập được, thông qua xử lý và chia sẻ lại của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) sẽ hỗ trợ cơ quan tổ chức khác có thể phòng, chống, ngăn chặn nguy cơ tấn công tương tự khi bị đối tượng tấn công sử dụng cùng mẫu mã độc, giúp tăng cường bảo đảm an toàn thông tin mạng.

Địa chỉ hệ thống kỹ thuật tiếp nhận thông tin: https://mis.ais.gov.vn, chi tiết về cổng kết nối và các thông tin khác liên hệ đầu mối kỹ thuật của Cục An toàn thông tin để được hướng dẫn kỹ thuật cụ thể theo thư điện tử: ais@mic.gov.vn; điện thoại: 02439436684.

3.2. Phương thức kết nối

Việc chia sẻ thông tin giữa máy chủ quản lý tập trung của các cơ quan đơn vị với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông được ký số và truyền đi qua kênh mã hoá HTTPS.

Thông tin chia sẻ bao gồm các trường được mô tả trong Phụ lục và đóng gói theo chuẩn edXML.

4. Nguyên tắc chia sẻ thông tin

Việc trao đổi và chia sẻ thông tin giữa máy chủ quản lý tập trung với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) tuân thủ nguyên tắc sau:

- Phù hợp với các quy định trong Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại và các quy định pháp luật liên quan khác.

- Thông tin chia sẻ giữa các tổ chức với Cục An toàn thông tin thực hiện qua kênh mã hoá và bảo đảm an toàn thông tin.

- Cục An toàn thông tin không chia sẻ thông tin riêng của các bên kết nối, cung cấp thông tin dữ liệu về mẫu mã độc với bên thứ ba.

- Thông tin chia sẻ định kỳ và thời điểm cập nhật thông tin do Cục An toàn thông tin xây dựng và thông báo đến các tổ chức để bảo đảm hiệu năng của hệ thống kỹ thuật.

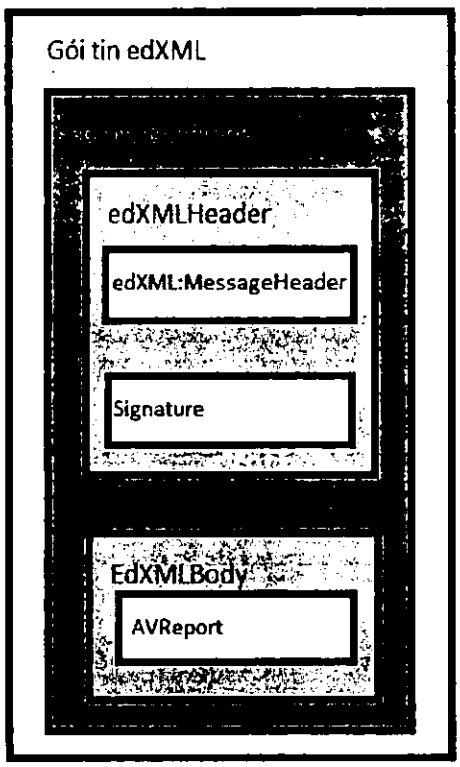
- Khi có thay đổi thông tin về máy chủ chia sẻ thông tin, các cơ quan đơn vị tổ chức thông báo về Cục An toàn thông tin để cập nhật kết nối chia sẻ.

5. Hướng dẫn về định dạng gói tin

5.1. Hướng dẫn định dạng gói tin edXML

Việc kết nối, chia sẻ thông tin giữa các hệ thống kỹ thuật, các hệ thống cần thực hiện trên cơ sở áp dụng định dạng dữ liệu trong gói tin edXML. Mục này quy định các yêu cầu kỹ thuật đối với các trường thông tin của gói tin edXML, không quy định về quy cách đóng gói gói tin edXML. Việc xác định quy cách đóng gói gói tin do các doanh nghiệp cung cấp giải pháp quyết định dựa trên cơ sở đáp ứng được các yêu cầu do các cơ quan có nhu cầu khai thác, sử dụng đặt ra.

Hình 1 mô tả cấu trúc cơ bản của một gói tin edXML gồm hai phần là thông tin cơ bản (edXMLHeader) và thông tin chính (edXMLBody).



Hình 1: Cấu trúc gói tin edXML

Phụ lục 1: Phần SOAP-ENV:Header

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.	**edXML:MessageHeader**		Đây là thông tin phải có của phần đầu gói tin, lưu trữ các thông tin về phần mở đầu và phần kết thúc của một báo cáo.	Bắt buộc	
1.1	edXML:From		Thông tin về đối tượng gửi báo cáo	Bắt buộc	
1.1.1	*edXML:OrganId*	Kiểu String Độ dài tối đa: 13	ID của cơ quan, tổ chức gửi báo cáo	Bắt buộc	QCVN 102:2016/BTTTT
1.1.2	*edXML:OrganizationInCharge*	Kiểu String Độ dài tối đa: 200	Tên cơ quan, tổ chức chủ quản trực tiếp (nếu có)	Tùy chọn	
1.1.3	*edXML:OrganName*	Kiểu String Độ dài tối đa: 200	Tên cơ quan, tổ chức gửi báo cáo	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.1.4	*edXML:OrganAdd*	Kiểu String Độ dài tối đa: 250	Địa chỉ của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.5	*edXML:Email*	Kiểu String Độ dài tối đa: 100	Thư điện tử liên lạc của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.6	*edXML:Telephone*	Kiểu String Độ dài tối đa: 20	Số điện thoại của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.7	*edXML:Fax*	Kiểu String Độ dài tối đa: 20	Số fax của cơ quan, tổ chức gửi báo cáo	Tùy chọn	
1.1.8	*edXML:Website*	Kiểu String Độ dài tối đa: 100	Trang/cổng thông tin điện tử của cơ quan, tổ chức gửi báo cáo	Tùy chọn	
1.2	edXML:Subject	Kiểu String Độ dài tối đa: 500	Trích yếu nội dung của báo cáo	Bắt buộc	
2	**Signature**		Mô tả về chữ ký số và thông tin ký số gói tin edXML	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
2.1	*SignedInfo*		Mô tả các thông tin được ký số	Bắt buộc	
2.1.1	*CanonicalizationMethod*		Xác định thuật toán chuẩn hóa dữ liệu cần ký số	Bắt buộc	Là một thuộc tính của *Canonicalization Method*
	Algorithm	Kiểu String	Thuật toán chuẩn hóa dữ liệu: http://www.w3.org/TR/xml-exc-c14n/		
2.1.2	*SignatureMethod*		Xác định thuật toán để ký số thành phần *SignedInfo* đã được chuẩn hóa	Bắt buộc	
	Algorithm	Kiểu String	Thuật toán ký số *SignedInfo*: http://www.w3.org/2000/09/xmldsig#rsa-sha1		Là một thuộc tính của *SignatureMethod*
2.1.3	*Reference*		Tham chiếu đến các đối tượng dữ liệu cần ký và xác định phương thức băm và giá trị băm của các thành phần đối tượng dữ liệu trong gói tin edXML	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	URI	Kiểu String	Tham chiếu đến đối tượng dữ liệu được băm. URI = "" tham chiếu đến *SOAP-ENV:Envelope*. URI = cid tham chiếu đến từng tệp dữ liệu đính kèm		Là một thuộc tính của *Reference*
2.1.3.1	*Transforms*		Danh sách phương thức biến đổi đối tượng dữ liệu định dạng XML được tham chiếu trước khi ký số	Bắt buộc	Chỉ sử dụng *Transforms* với đối tượng SOAP-ENV:Envelope (XML)
	Transform		Định nghĩa một phương thức biến đổi sẽ được áp dụng	Bắt buộc	
	Algorithm	Kiểu String	Tên phương thức biến đổi được áp dụng. Có các loại sau: - Sử dụng Enveloped Signature: www.w3.org/2000/09/XMLDSig#enveloped-signature - Sử dụng thuật toán chuẩn hóa nội dung XML, XML-C14N: www.w3.org/TR/xml-exc-c14n/		Là một thuộc tính của *Transforms*

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
2.1.3.2	*DigestMethod*		Xác định thuật toán băm dữ liệu http://www.w3.org/2001/04/xmlenc#sha256	Bắt buộc	
	Algorithm	Kiểu String	Thuật toán băm dữ liệu		Là một thuộc tính của *DigestMethod*
2.1.3.3	*DigestValue*	Kiểu String	Giá trị băm của đối tượng dữ liệu tham chiếu sử dụng thuật toán quy định tại *DigestMethod*	Bắt buộc	
2.2	*SignatureValue*	Kiểu String	Giá trị chữ ký số của *SignedInfo*	Bắt buộc	
2.3	*KeyInfo*		Mô tả khóa sử dụng để xác thực chữ ký số	Bắt buộc	
2.3.1	*X509Data*		Dữ liệu về chứng thư số sử dụng để xác thực chữ ký số	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
2.3.1.1	*X509SubjectName*	Kiểu String	Tên cá nhân/tổ chức ký số	Bắt buộc	Tên cá nhân/tổ chức sở hữu chứng thư số ký
2.3.1.2	*X509Certificate*	Kiểu String	Chứng thư số sử dụng để xác thực chữ ký số	Bắt buộc	

Phụ lục 2: Phần SOAP-ENV: Body

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1	**AVReport**		Các thông tin báo cáo của Anti Virus	Bắt buộc	
	name	Kiểu String	Tên của Anti Virus gửi báo cáo	Bắt buộc	
1.1	**Datetime**	Kiểu string	Thời gian gửi báo cáo	Bắt buộc	Sử dụng Unix time
1.2	**Malware**		Báo cáo thông tin mã độc trên các máy	Bắt buộc	Nếu không có mã độc thì nội dung bỏ trống, nếu có thì **bắt buộc** phải có các thẻ bên trong.
1.2.1	**Machine**		Thông tin về mã độc trên từng máy	Bắt buộc	Bỏ qua nếu không có thông tin mã độc

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	ip	Kiểu string	Địa chỉ IP của máy nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
	ippublic	Kiểu string	Địa chỉ IP public của máy tính bị nhiễm mã độc	Tuỳ chọn	Bỏ qua nếu không có thông tin mã độc
	name	Kiểu string	Tên máy nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1	**MalwareInfo**		Các thông tin về mã độc trên máy	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.1	**MalwareName**	Kiểu string	Tên mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.2.1.1.2	**MalwareType**	Kiểu string	Loại mã độc (PE, Trojan, spyware, worm, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.3	**MalwareBehavior**	Kiểu string	Hành vi của mã độc (Downloader, Dropper, CoinMiner, Keylogger, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.4	**TypeOfDevice**	Kiểu string	Loại thiết bị nhiễm mã độc (USB, HDD, SDCard, SSD, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.5	**NumberFile**	Kiểu integer	Số lượng tập tin bị nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.3	**Connection**		Thông tin kết nối nghi ngờ.	Bắt buộc	Nếu không có connection lạ thì các trường bên trong bỏ trống. Nếu có thông tin Connection thì các trường bên trong **bắt buộc** phải có.
1.3.1	**Machine**		Thông tin kết nối nghi ngờ trên từng máy	Bắt buộc	Bỏ qua nếu không có thông tin connection
	ip	Kiểu string	IP của máy có kết nối nghi ngờ	Bắt buộc	Bỏ qua nếu không có thông tin connection

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	ippublic	Kiểu string	Địa chỉ IP public của máy tính bị nhiễm mã độc	Tuỳ chọn	
	name	Kiểu string	Tên của máy có kết nối nghi ngờ.	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1	**ConnectionInfo**		Thông tin kết nối nghi ngờ	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1.1	**Program**	Kiểu string	Tên chương trình có kết nối nghi ngờ.	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1.2	**TargetIP**	Kiểu string	IP đích của kết nối nghi ngờ.	Tuỳ chọn	Bỏ qua nếu không có thông tin connection

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.4	**Vulnerability**		Thông tin lỗ hổng trên các máy	Bắt buộc	Nếu không có lỗ hổng nào trên các máy thì các trường bên trong bỏ trống. Nếu có lỗ hổng thì các trường bên trong **bắt buộc** phải có.
1.4.1	**Machine**		Thông tin lỗ hổng trên từng máy	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
	ip	Kiểu string	Địa chỉ IP của máy có lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	ippublic	Kiểu string	Địa chỉ IP public của máy tính có lỗ hổng	Tuỳ chọn	Bỏ qua nếu không có thông tin lỗ hổng
	name	Kiểu string	Tên của máy có lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1	**VulnerabilityInfo**		Các thông tin về lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1.1	**Name**	Kiểu string	Mã CVE của lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1.2	**OSName**	Kiểu string	Tên hệ điều hành của máy có lỗ hổng	Tuỳ chọn	Bỏ qua nếu không có thông tin lỗ hổng.

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.5	**OS**		Thông tin hệ điều hành của các máy	Bắt buộc	
1.5.1	**Machine**		Máy có báo cáo thông tin hệ điều hành	Bắt buộc	
	ip	Kiểu string	IP của máy có báo cáo thông tin hệ điều hành	Bắt buộc	
	ippublic	Kiểu string	Địa chỉ IP public của máy tính có báo cáco thông tin hệ điều hành	Tuỳ chọn	
	name	Kiểu string	Tên của máy có báo cáo thông tin hệ điều hành	Bắt buộc	
1.5.1.1	**OSName**	Kiểu string	Tên hệ điều hành	Bắt buộc	
1.5.1.2	**LastUpdate**	Kiểu string	Thời gian cập nhật hệ điều hành mới nhất	Bắt buộc	Định dạng Unix time
1.6	**Update**		Thông tin tình hình cập nhật của các máy	Bắt buộc	
1.6.1	**NumberMachineNotUpdate On15Day**	Kiểu Interger	Số máy không được cập nhật trong vòng 15 ngày.	Bắt buộc	Tất cả máy được update ≤ 15 ngày thì dữ liệu ghi 0.

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.7	**QualityFeature**		Thông tin trạng thái bật tắt của những tính năng quan trọng	Bắt buộc	
1.7.1	**Machine**		**Máy có báo có thông tin trạng thái bật tắt của những tính năng quan trọng**		
	ip	Kiểu string	IP của máy	Bắt buộc	
	Name	Kiểu string	Tên máy	Bắt buộc	
1.7.1.1	**AutoProtect**	Kiểu string	Trạng thái tính năng tự động bảo vệ thời gian thực (On, Off)	Bắt buộc	
1.7.1.2	**EnableFirewall**	Kiểu string	Trạng thái của firewall (On, Off)	Bắt buộc	

Phụ lục 3: Ví dụ về một gói tin edXML

```
<edXMLEnvelope xmlns:edXML= "http://www.mic.gov.vn/
TBT/QCVN_102_2016">
   <edXML:edXMLHeader>
      <edXML:MessageHeader>
         <edXML:From>
            <edXML:OrganId>00.01.H26</edXML:OrganId>
            <edXML:OrganName>ĐOn vị gửi report </edXML:OrganName>
            <edXML:OrganAdd> Địa chi - Hà Nội</edXML:OrganAdd>
            <edXML:Email>email@abc.gov.vn</edXML:Email>
            <edXML:Telephone>(043)22222222</edXML:Telephone>
            <edXML:Fax>(043)22222222</edXML:Fax>
            <edXML:Website>http://website.gov.vn</edXML:Website>
         </edXML:From>
         <edXML:Subject>Anti Virus Report on 12-06-2018</edXML:Subject>
      </edXML:MessageHeader>
      <Signature xmlns= "http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm= "http://www.w3.org/2001/10/xml-
exc-c14n#" />
        <SignatureMethod Algorithm= "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
        <Reference URI="">
          <Transforms>
            <Transform Algorithm=
"http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            <Transform Algorithm= "http://www.w3.org/TR/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="
http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>PuRChYEMCsAVya7V39ybDhGodNKDo8OTQtOOUwtx4B5=
</DigestValue>
        </Reference>
      </SignedInfo>
<SignatureValue>FXM4QWgcX3Eb0fdB+p50Kh9p4jhnc2rIzvun5+FRlQ2ruCClXQKGMbupEq3
qXpTXNxxHcD/euv+RFH2EgIbyh070uj6lIW4zlfZAuVtOkMjbgVLjoTyy9xtqc+PXcmUO8vqX7o
yzR7MLK5JCkIsDUD0PNIxD7l8kFFqqVfvhvb4RL466YBEh2m48gbDzkWizBis6sFHXzQH20ACc9
ko39NPiPNfcKjG0f/q4/esbPPyzOUTcdRMW6+hTI6aPFb8jn/MSS43VE4TbiDJIllWkmULnLspC
lMzTMEaKba5Cq7NvoIRif9E5NK316WYA7hponYI6kyLCdJxoOZEtOnSPQr==</SignatureValu
e>
      <KeyInfo>
        <X509Data>
          <X509SubjectName>CN=user05, L=Ha Noi, O=Ban Co yeu Chinh phu,
OU=Cuc Quan ly Ky thuat Nghiep vu Mat Ma, OU=Trung tam chung thuc dien tu
chuyen dung Chinh phu, C=VN</X509SubjectName>

<X509Certificate>MIIFqTCCBJGgAwIBAgIDLfAwMA0GCSqGSIb3DQEBBQUAMFYxCzAJBgNVBA
YTAlZOMR0wGwYDVQQKDBRCYW4gQ28geWVlIENoaW5oIHBodTEoMCYGA1UEAwwfQ28gcXVhbiBja
HVuZyB0aHVjIHNvIENoaW5oIHBodTAeFw0xMTA0MTMwOTQyMzlaFw0xNjA0MTEwOTQyMzlaMIG7
MQswCQYDVQQGEwJWTjE7MDkGA1UECwwyVHJ1bmcgdGFtIGNodW5nIHRodWMgZGllbiB0dSBjaHV
5ZW4gZHVuZyBDaGluaCBwaHUxLjAsBgNVBAsMJUN1YyBRdWFuIGx5IEt5IHRodWF0IE5naGllcC
B2dSBNYXQgTWExHTAbBgNVBAoMFEJhbiBDbyB5ZXUgQ2hpbmggcGh1MQ8wDQYDVQQHDAZIYSBOb
2kxDzANBgNVBAMMBnVzZXIwNTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMh/+mvm
2ev1584e1fzXE1cfzTK5GuCmA9r74UkDfbiP+4MedIQ/k2pyL2mzM50sbpx+0AeRBSO0xIrb2yV
sKmKC8JSzub8JLUhbyvtnh5rFLphBPRAi+MNvSZXByWDKvGHt8NwPGspNsgL1AI0bmz0GksOxiR
mil6mo/7YWFKBUCTkYB9a/pnLofJeBy/zQ2ekw6oUF5CNJq9t/MLXmP2s3AVdq4KR2PJ3xRiSUF
Kat9RBcgR5Qi+NbvuURsWnloYysWiyFMd6ifWSouocOb/T33Xlp+IVz6GaFfVwYQ299TEDVHqXQ
Zg7KkfMenkQgyKe2jOIJBAI3pyLhcanS0t8CAwEAAaOCAhgwggIUMAkGA1UdEwQCMAAwCwYDVR0
PBAQDAgZAMCUGCWCGSAGG+EIBDQQYFhZVc2VyIFNpZ24gb2YgQ2hpbmggcGh1MB0GA1UdDgQWBB
T7mk6fmUv19ktMqjSzTsyIbRuIGTCBlQYDVR0jBIGNMIGKgBQFMUDeNL6zj8DbbsVDDj4S92PGH
```

```
KFvpG0wazELMAkGA1UEBhMCVk4xHTAbBgNVBAoMFEJhbiBDbyB5ZXUgQ2hpbmggcGh1MT0wOwYD
VQQDDDRDbyBxdWFuIGNodW5nIHRodWMgc28gY2h1eWVuIGR1bmcgQ2hpbmggcGh1IChSb290Q0E
pggEEMBsGA1UdEQQUMBKBEHVzZXIwNUBjYS5nb3Yudm4wMgYJYIZIAYb4QgEEBCUWI2h0dHA6Ly
9jYS5nb3Yudm4vcGtpL3B1Yi9jcmwvY3AuY3JsMDIGCWCGSAGG+EIBAwQlFiNodHRwOi8vY2EuZ
292LnZuL3BraS9wdWIvY3JsL2NwLmNybDBjBgNVHR8EXDBaMCmgJ6AlhiNodHRwOi8vY2EuZ292
LnZuL3BraS9wdWIvY3JsL2NwLmNybDAtoCugKYYnaHR0cDovL3B1Yi5jYS5nb3Yudm4vcGtpL3B
1Yi9jcmwvY3AuY3JsMDIGCCsGAQUFBwEBBCYwJDAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AuY2
EuZ292LnZuLzANBgkqhkiG9w0BAQUFAAOCAQEAbsHix/XUcD7i+p5ufYNVxxYk0J/guTxE6t9fb
gPvMcpxQrUu9JpHmNkna/r/OvEm2ply1aAb60DHaC196nU17pt6HBMJt80X36RDUpghnkmmc3C6
XZwCBve8A45WByYv+FNIEDpNoGgjZ2T5wpwWnq9w4d4Nnb5R4EZGZ7zKEu/JLo1VuH0gAM1KyVE
1Qj3hEwHYbZDQHlsBXZURtmS89F33xcadMDny3ymoiPH9f7MMBSwmgDISnHCDgyBijJo3m9tQV2
SeuLs6NxNWnFKkOWTISLrpTzEkbChYR1z4t/nIvJ7j0rwgRB+gWFxgYGj8HxcZMy8Xv9cy+f4Xd
xxxxx==</X509Certificate>
        </X509Data>
      </KeyInfo>
    </Signature>
  </edXML:edXMLHeader>
  <edXML:edXMLBody>
      <AVReport name= "Anti-Virus Name ">
          <Datetime>1530530315</Datetime>
          <Malware>
              <Machine ip = '10.2.44.2' name = 'XD-ABVCDFGF'>
                  <MalwareInfo>
                      <MalwareName>W32.BitminerTTc.trojan</MalwareName>
                      <MalwareType>Trojan</MalwareType>
                      <MalwareBehavior>CoinMiner</MalwareBehavior>
                      <TypeOfDevice>HDD</TypeOfDevice>
                      <NumberFile>10</NumberFile>
                  </MalwareInfo>
                  <MalwareInfo>
                      <MalwareName>W32.FakeFolder.Worm</MalwareName>
                      <MalwareType>Worm</MalwareType>
                      <MalwareBehavior>Keylogger</malwareBehavior>
                      <TypeOfDevice>USB</TypeOfDevice>
                      <NumberFile>1</NumberFile>
                  </MalwareInfo>
              </Machine>
          </Malware>
          <Connection>
              <Machine ip = '10.2.44.3' name = 'XD-HTDmachine'>
                  <ConnectionInfo>
                      <Program>avcd.exe</Program>
                      <md5>39E97D1D9EA2BB19604F16020B246B2D</md5>
                      <Sha2>
2d70aec10567f263f9f4ad08e49439c0bf014529a1a92739c2845e556fee8b3e
                      </Sha2>
                      <TargetIP>103.90.90.2</TargetIP>
                  </ConnectionInfo>
                  <ConnectionInfo>
                      <Program>tknss.exe</Program>
                      <md5>F9D2868315D16295609640731FD74BB5</md5>
                      <TargetIP>110.30.3.10</TargetIP>
                  </ConnectionInfo>
              </Machine>
          </Connection>
          <Vulnerability>
              <Machine ip = '10.2.44.3' name = 'XD-ACKGHTD'>
                  <VulnerabilityInfo>
                      <Name>CVE-2008-1234</Name>
                      <OSName>Windows 7</OSName>
                  </VulnerabilityInfo>
              </Machine>
          </Vulnerability>
          <OS>
```

```
                <Machine ip = '10.2.44.3' name = 'XD-ACKGHTD'>
                    <OSName>Windows 7</OSName>
                    <LastUpdate>18-06-2018</LastUpdate>
                </Machine>
            </OS>
            <Update>
            <NumberMachineNotUpdateOn15Day>10</NumberMachineNotUpdateOn15Da
            y>
            </Update>
            <QualityFeature>
                <Machine ip = '10.2.44.3' name = 'XD-ACKGHTD'>
                    <AutoProtect>Off</AutoProtect>
                    <EnableFirewall>Off</EnableFirewall>
                </Machine>
            </QualityFeature>
        </AVReport>
    </edXML:edXMLBody>
</edXMLEnvelope>
```