HƯỚNG DẪN PHÁT HIỆN THƯ GIẢ MẠO

1. Phương thức tạo thư giả mạo của tin tặc

Thông thường khi soạn và gửi thư điện tử, người gửi thư chỉ biên soạn nội dung, tiêu đề thư (title), địa chỉ nơi nhận, lựa chọn các tệp tin đính kèm, các thông tin còn lại khác sẽ do máy chủ gửi thư tự động cập nhật như: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lại (Reply-To) và địa chỉ hòm thư người gửi (from).

Để đánh lừa người nhận tin, bước đầu tin tặc sẽ tìm cách tự biên soạn thư điện tử với các thông tin giả mạo về: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi (from). Sau đó tin tặc sẽ tìm một máy chủ thư điện tử hoặc tự cài đặt một phần mềm gửi thư (MTA) không yêu cầu xác thực hòm thư người gửi để phát tán thư điện tử giả mạo tới người cần lừa đảo.

2. Tìm hiểu nguồn gốc thật phát tán của thư điện tử

Trong nội dung thư điện tử gửi đến người nhận bao gồm các đầy đủ thông tin về: địa chỉ IP của máy gửi thư; địa chỉ hòm thư nhận; địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi (from); nội dung thư; Tiêu đề thư; Các tệp tin đính kèm. Nhưng trong chế độ hiển thị thông thường (mặc định) để đơn giản hóa giao diện, hầu hết các chương trình duyệt thư điện tử chỉ hiện các thông tin: địa chỉ hòm thư tiếp nhận thư trả lời (Reply); Đia chỉ hòm thư người nhân; nôi dung thư; tiêu đề thư; các têp tin đính kèm và các thời gian liên quan. Các thông tin chi tiết về nguồn gốc của thư như: địa chỉ IP của máy gửi thư; đia chỉ hòm thư nhân phản hồi khi thư bi trả lai (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi (from) được lưu trong phần đầu (header) của thư sẽ chỉ hiện thi chi tiết khi người nhân thư sử dụng các chức năng cho xem nguồn gốc (original) của thư hoặc xem nội dung phần đầu (header) của thư (Chú ý: đối với mỗi trình duyệt và hệ quản trị thư điện tử khác nhau sẽ có những cách khác nhau để xem nguồn gốc của thư điện tử, tuy nhiên tất cả các phần mềm trên đều hỗ trợ chức năng show original). Cách xem nguồn gốc thư điện tử của một số hệ thống thư điện tử phổ biến sẽ được trình bày trong Phu lục A

3. Phát hiện thư giả mạo

Qua phân tích các thư điện tử giả mạo đã gửi đến các cơ quan nhà nước trong thời gian vừa qua, có hai dấu hiệu chính để có thể phát hiện ra các thư giả mạo theo phương thức này là:

1. Khi mở xem nguồn gốc chi tiết của thư điện tử, địa chỉ hòm thư "Return-Path" không trùng với địa chỉ hòm thư người gửi đến (From). Hầu hết các thư điện tử được gửi từ các hệ thống thư điện tử của cơ quan nhà nước (có đuôi .gov.vn) đều có hai địa chỉ này trùng nhau.

2. Địa chỉ IP của máy chủ gửi thư không trùng với địa chỉ IP của hệ thống thư điện tử thật nơi bị giả mạo là gửi thư điện tử. Hiện nay, các địa chỉ IP giả mạo này thường có nguồn gốc từ nước ngoài trong khi địa chi IP các hệ thống cơ quan nhà nước thường có địa chỉ IP trong nước.

Ví dụ minh họa :

Dưới đây là ví dụ minh họa một thư điện tử giả mạo ông Vũ Xuân Hoàng có địa chỉ thư điện tử là <u>hoangvx@abc.gov.vn</u> được tin tặc gửi tới hòm thư của chị Nguyễn Thanh Huyền có địa chỉ <u>huyennt@xyz.gov.vn</u>. Tin tặc tạo ra thư giả mạo ông Vũ Xuân Hoàng có tiêu đề là "Thông báo lớp đào tạo" với các địa chỉ hòm thư gửi, và hòm thư nhận là hoangvx@abc.gov.vn, hòm thư trả lại là root@nbr.com. Sau đó tin tặc sử dụng máy gửi thư có địa chỉ IP xxx.xxx.xxx để gửi thư giả mạo đã soạn tới hòm thư của chị Nguyễn Thanh Huyền có địa chỉ <u>huyennt@xyz.gov.vn</u>.

Địa chỉ hòm thư trả lại - Return
Received: from xyz.gov.vn (LHLO xyz.gov.vn) (yyy.yyy.yyy) by xyz.gov.vn with
LMTP; Sat, 18 May 2013 15:24:12 +0700 (ICT)
Received: from localhost (localhost by xyz.gov.vn (Postfix) with for <huvennt@xyz.gov.vn>; Sat, to may zota (12,111, 10,00, 110)</huvennt@xyz.gov.vn>
Received: from nbr.com (unknown [xxx.xxx.xxx]) by xyz.gov.vn Postfix) with ESMTP id C4493288FE8 for <huyennt@xyz.gov.vn> Sat, 18 May 2013 15:23:43 +0700 (ICT)</huyennt@xyz.gov.vn>
Date: Sat, 18 May 2013 12:25 Message-Id: <201305181625 Dia chỉ hòm thư nhận cần lừa đảo
To: huyennt@xyz.gov.vn Subject: Thông báo lóp đảo tạo Địa chỉ hòm thư gửi (bị giả
From: Vu Xuan Hoang <hoangvx@abc.gov.vn></hoangvx@abc.gov.vn>
Reply-To: hoangvx@abc.gov_vn Địa chỉ hòm thư nhận trả lời (bị giả mạo)

4. Báo cáo khi nhận được thư giả mạo

Khi phát hiện được thư giả mạo, đề nghị gửi thư giả mạo theo hình thức dưới dạng tệp tin đính kèm (attachment hoặc forward as attachment) tới địa chỉ <u>duythanh@tayninh.gov.vn</u>. Cách gửi thư giả mạo dưới dạng tập tin đính kèm sẽ được trình bày trong <u>Phụ lục B</u>.

Để gửi thông tin về cho chúng tôi xin vui lòng làm theo mẫu sau sau:

	Địa chỉ: duythanh@ta	yninh.gov.vn
	Tiêu đề: Báo cáo thư	giả mạo
	Nội dung:	
	Báo cáo thư giả mạo.	
	Tên người gửi:	Nguyễn Văn A
	Địa chỉ Email liên lạc	c:nva@zyx.gov.vn
	Số điện thoại liên hệ:	09xxxxxxx
XXX	Thông tin chi tiết về Với nội dung lừa đảo d	vấn đề: Tôi nhận được email nghi vấn giả mạo từ địa chỉ để tôi gửi thông tin về lãnh đạo cơ quan

Tập tin đính kèm chứa nội dung nguyên bản (chứa đầy đủ phần đầu của thư điện tử): msg001.mail

Phụ lục A : Hướng dẫn hiển thị tiêu đề của thư điện tử

1. Phần mềm Microsoft Outlook 2010 và các phiên bản mới hơn:

Kích đúp vào tin nhắn để mở ra cửa sổ mới. Từ thanh công cụ -> tab **Message** -> kích vào ô nhỏ có hình mũi tên trong khung **Tags** hoặc **Options**

File	/lessage						۵ 🕜
ि X & ▼ Delete	Reply	Completed Tasks To Manager Team E-mail	*	Move	🗟 Mark Unread III Categorize ▼ ▼ Follow Up ▼	a ∰ Translate	Zoom
Delete	Respond	Quick Steps	5	Move	Tags 🕞	Editing	Zoom

Cửa số **Properties** mở ra và hiển thị phần tiêu đề thư:

Properties	×					
Settings	Security					
Importance Sensitivity:	Normal Normal Normal Request S/MIME receipt for this message					
Do not Au	utoArchive this item					
Tracking options Request a delivery receipt for this message Request a read receipt for this message						
Delivery options						
Have replies	sent to:					
Expires a	fter: None < 12:00 AM <					
Contacts						
Categories 🔻	None					
Internet headers: Microsoft Mail Internet Headers Version 2.0 Received: from smtpanon.uidaho.edu ([129.101.177.61]) by EXVS2.its.uidaho.edu with Microsoft SMTPSVC(6.0.3790.4675); Thu, 14 Jul 2011 16:11:35 -0700 Received: from proofagent2.uidaho.edu ([129.101.155.252]) by smtpanon.uidaho.edu with Microsoft SMTPSVC(6.0.3790.4675); Thu, 14 Jul 2011 16:11:35 -0700						
	Close					

2. Phần mềm Microsoft Outlook các phiên bản trước 2010:

Kích phải vào tin nhắn muốn hiển thị và chọn Message Options

Arrang	ed By	r: Date	Newest on top	-	
🖃 Тос	day				
🖂 lis Gi		<u>O</u> pen	Ì	5:59 p.m.	8
科 Va	÷	<u>P</u> rint		5:20 p.m.	7
G	2	<u>R</u> eply		0.70	
NO NO	2	Reply to A <u>l</u> l		8:39 a.m.	8
🖂 lo	2	For <u>w</u> ard	o.nz	4:02 a.m.	~
Lo		Follow Up	0		
🖻 Ar	\square	Mar <u>k</u> as Read		3:45 a.m.	7
		Find <u>A</u> ll			
🖃 Ye	1	Create Rule			
🖂 La		Junk E-mail	lav lune 15	Wed 10:24 a.m.	7
🖂 La		ESET Smart Security		Wed 9:21 a.m.	∇
La	\times	<u>D</u> elete	une 15		
	6	Move to Folder			
	:	Message Ogtions 🖊			

Sau đó cửa sổ Properties chứa tiêu đề thư sẽ được hiển thị.

3. Phần mềm Thunder Bird :

Mở tin nhắn chọn "View" sau đó chọn "Message Source" hoặc Headers -> All:



4. Phần mềm Apple Mail :

Mở tin nhắn chọn "**View**" trên thanh menu sau đó chọn "**Message**", tiếp đó chọn **All Header** hoặc **Raw Source**



5. Webmail với hệ quản trị email Zimbra:

Ân chuột phải vào thư điện tử cần xem. Lựa chọn mục Show Original:

]		Search				🖂 Mail 👻
		New	C Get Mail X Dele From Iran M. mang Ngo T. M. Su, Tran M. Thang	 G Find Emails Advanced Search New Email Edit Contact Forward Contact 	• [nm]	Reply 🛃 Reply to A
			Diep Tuan. Mi	~		ort email - Hi Phú, Hiệi
			Bui T Minh. H	😡 Mark As Read	[mr]	khai học tập, quán tri
			Phung L. Anh	🖂 Mark As Unread	[mu]	ợp báo cáo ATTT của
			Hoang, Nguy			ần sử dụng trên máy
Ś	E	Issue of rep	oort email	🔁 Reply	[r]	
		- From:	Diep Tuan, Minh	😒 Reply to All	[a]	
				🖂 Forward	[f]	
		IO: Ng	guyen H. Phu	🥖 Edit as New		
		Hi Phú,		-		
		Hiện tại	Minh không đăng	V Delete		eport@vncert.
		Phúc có t	thể chock lại dùm		[Del]	lai bôn mail .
		Phue co t	the check lại dum	Move		lại nộp maii i
				🖶 Print	[q]	
		Diep Tuar	n Minh Computer Emergenc			
		vietnam (computer intergent	27 Mark as Spam	[ms]	[
_				Show Original		
-				🕂 New Filter		
						-

6. Đối với Webmail của Gmail

Sau khi mở email cần hiển thị ta kích vào mũi tên nhỏ bên phải và kích vào "hiển thị thư gốc":

Gmail -	← D D D	Tác vụ khác 🗸	1 trong
SOẠN	Mobile Ads Drain Batteries Microsoft Buil	d: 3 Windows 8 Questions	Hộp thư đến x
Hộp thư đến Thư gắn dấu sao Quan trọng Thư đã gửi Thư nháp (1) Spam (15) Vàng kết đấi 100	InformationWeek Daily IWKBTnewsletters@techweitöri töi T Hinh ành không được hiển thị. Hiến thị hình ảnh dữ Tiếng Anh → > Tiếng Việt → Dịch thư	o.com <u>qua</u> info.blackhatcovertchannel rới đây - Luôn hiến thị hình ảnh từ IV	.com 00:31 (14 giờ trước) ☆ ✓
[Imap]/Drafts [Imap]/Trash	InformationWeek Daily	you have trouble viewing this email, <u>read the o</u>	Them InformationWeek Daily vao Danh sach lien ne Xóa thư này Báo cáo spam Báo cáo spam Hiển thị thự gốc
Tìm kiếm, trò chuyệr • nguyen lanhuong • softprovietnam	InformationWeek Daily Wednesday, June 26, 2013 N	ews <u>Commentary</u> <u>Slideshows</u> <u>Re</u>	Nội dung thư hiển thị không đúng? Đánh dầu là chưa đọc corts <u>Videos</u> <u>Events</u> <u>RSS Feeds</u>
Bui Xuan Giao	MUST READ	010	TE OF THE DAY

7. Đối với Webmail của Yahoomail

Thực hiện lựa chọn tin nhắn cần hiển thị. Chọn nút "**Thao tác**" trên thanh công cụ -> "**Xem tiêu đề đầy đủ**" để hiển thị tiêu đề thư:

À	LICH	Adobe Creative Clou				
Ī	🗍 Xóa	★ ★ →	💽 Chuyến 🚽	🗿 Thư rác 🚽	🍄 Thao tác 👻 🔹 🔹 🐥	
- <i>I</i>	Adobe C	Creative Cloud: Please v	verify your email addr	In Thư	Pinnie	
	Từ /	Adobe Creative Cloud +			Đánh dấu Đã đọc	к
	Den	VETR_901@TAHOO.COM			Đánh dấu Chưa đọc	Shift+K
					Đánh dấu sao	L
	(S Adobe Creative	Cloud™		Xóa đánh dấu sao	Shift+L
					Xem tiêu đê đây đủ	
You're almost there!					Cài bảng mã ngôn ngữ	
					Thêm Người gửi vào Danh bạ	Shift+A
	Н	li phu,				
	-					

8. Đối với Webmail Tây Ninh

Thực hiện mở tin nhắn cần hiển thị, chọn nút "Mở rộng" (More), chọn tiếp "Show MIME Header" hoặc "Show MIME Full"

e mail.tayninh.gov.vn/m	ail/duythanh.nsf?Open		습 [.]
IBM Lotus. iNotes.			
🛓 Thư-Hộp thứ 🗙 🗟 test	tu mail ya X		
🤞 📸 🔜			
duythanh PB1/TAYNINH	🕈 Tạo mới 🔹 🚝 Trả lời 🔹 买 Trả lời cho tất cả 🔹 🗟 Chuyển tiếp 🔹 📄 🔹		Mở rộng 🔻 😝
Hộp thự đến (185)	tes Vuo Chon muc Mở rông		Tùy chọn Đi công tác
 Họp thứ đen (185) Bản thảo Thư đã gửi Thư đã gửi Theo dõi Tất cả tài liêu 	Tới: test		Sao chép tới Thêm người gửi vào địa chỉ liên hệ Chặn thư từ người gửi Lập lịch họp
20 Thư rác 11 Thùng rác 11 Thư mục	Vuc Phó	g tin và Tr	Tạo mới thư từ thư mẫu Tạo mới mẫu thư Xem mẫu thư
n Công cụ Ng Hộp thư khác	Sở 1 Chọn Snow IVIIIVIE Header Ema ĐT:	p2, tx Tây	Thông tin phân phối thư Tạo nhanh Luật lọc thư Luật lọc thư Tạo mới Luật lọc thư
	L		Show MIME Header Show MIME Full

Phụ lục B : Hướng dẫn gửi thư giả mạo dưới dạng tệp

1. Đối với Outlook 2010

Lựa chọn tin nhắn muốn gửi đi. Lựa chọn tab "**Home**" trên thanh công cụ. Trong mục "**Respond**" chọn "**More**"->"**Forwardas Attachment**"

I I File Home Send / Receive	Folder View	Inbox -	- Microsoft Outlook
New New E-mail Items - New Delte	Repty Repty Forward Forward Repty Ac Delte Repty Ac	Move Rules OneNote Kove Tags	Find a Contact M Address Book Filter E-mail Find
Favorites Inbox (1) Information	C Search Int ! 泣 D @ From Subject	pox (Ctrl+E)	For tonight - next ema
Sent Items	Date: Two Weeks Ago	E T	ent: Wed 10/3/2012 11:17 AM
 @sheridancollege.ca Tabox (1) 	For tonight - next email will list tomorrow night's group FileMaker, FileMaker Web Seminar	Wed 10/3/201 19 KB	

2. Đối với Outlook 2007

Lựa chọn tin nhắn muốn gửi. Lựa chọn "Action" menu và kích vào "Forward as Attachment"



3. Đối với Thurnderbird

Lựa chọn tin nhắn, menu "Message" -> Foward As -> Attachment.

Inbox for akimov@cern	.ch - Thunderbird	ł							×
<u>File Edit View G</u> o	Message Tool	ls <u>H</u> elp							
Get Mail Write Add	<u>N</u> ew Message <u>R</u> eply	Ctrl+N Ctrl+R	Rag -	X Delete	M Junk F	Sint -	Government of the second secon	✓ Subject or Sender	
All Folders	Reply to All	Ctrl+Shift+R					68 Sender	M Date	- E
akimov@cern.ch	<u>F</u> orward	Ctrl+L	L	_			Christian Isnard	- 05/08/2010 09:12	~
Inbox	For <u>w</u> ard As	►	Inline				 Emmanuel Ormancey 	 05/08/2010 09:32 	
- Sent	Edit Message	As New Ctrl+E	<u>A</u> ttachmer	nt			 akimov 	 05/08/2010 09:50 	
- 🗍 Trash	<u>O</u> pen Messag	e Ctrl+O					 Andrei Akimov 	 05/08/2010 10:07 	
- 🔜 Deleted Messages	Maure		CERN accou	nt page			 Michal Budzowski 	 05/08/2010 11:18 	
- Sent Messages	IVIOVE		e on CERN ac	count page			 Michal Budzowski 	 05/08/2010 11:27 	
🗉 🔄 Local Folders	Copy	•	e on CERN ac	count page			 Emmanuel Ormancey 	 05/08/2010 11:30 	E
	Move Again	Ctrl+Shift+M	5 reports				 Alexey Tselishchev 	 05/08/2010 12:40 	
	Tag	•	5 reports				 Jaroslaw Polok 	 05/08/2010 13:45 	
	Mar <u>k</u>	•	ncement				 Christian Boissat 	 05/08/2010 14:44 	
			·				Anton Akimov	 05/08/2010 15:24 	
	Create Filter F	rom Message	A HATY (0031	R-0017) Po	rtable com	puter r	 noreply@cern.ch 	 05/08/2010 16:52 	
	-	II-OIS Group Re	eport for CS-06	-Aug-2010			Christian Isnard	 05/08/2010 18:09 	-
	-	Re: At home too	dav				 Jurai Sucik 	· 06/08/2010 07:46	
		Subject: test							
		From: akimov							
		Date: 05/08/2010 0	19:50						
		lo: <u>akimov@cer</u>	<u>m.ch</u>						
	tes	st							
8								Unread: 0 Total	: 25

4. Đối với Apple Mail

Click chuột phải vào tin nhắn muốn gửi và lựa chọn "Forward as Attachment"

Sort by Date 🔻		
InformationV Mobile Ads Dra If you have email, reac hongphul Website is http://www.	Veek Daily 12:31 AM ain Batteries Micro Open Reply Reply All Forward Forward as Attachment	From: InformationWeek Daily Subject: Mobile Ads Drain Batteries I Microsoft B Te: June 27, 2013 12:31:01 AM GMT+07:00 To: hongphukt@gmail.com To: InformationWeek Daily
hongphul Website is http://www.	Redirect Mark Delete	formation
Information CIA Picks / If you have email, read	Flag: × 🏴 🏴 🏴 🏘 🖗 🖗	Sday, June 26, 2013
noreply@ Snort.org p Please visi your passv	Archive Move To Copy To Copy to "Tất cả thư" Again	READ Microsoft Build: 3 Windows By Michael Endler Microsoft has a chance to regain contro conference. But can the company execu
Cool Clouc	Apply Rules	TED ows 8.1: 10 Surprise Benefits

5. Đối với Gmail và Yahoo

Ta cần phải hiển thị thư gốc ra như hướng dẫn 6 và 7 ở <u>Phụ lụ c A</u> và lưu chúng lại thành một tập tin dạng văn bản.



Sau đó thực hiện gửi email đính kèm tập tin văn bản đó cho chúng tôi.