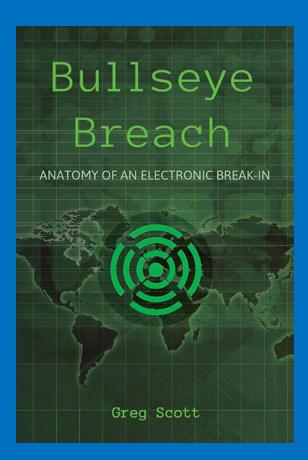
Deconstructing a spam email



Greg Scott

🔤 🖬 ち び 🋧 🎍 🕫		Boost your reputation of excellent lover - Message (Plain Text)				? 🗹	– 🗆 🗙
FILE MESSA	GE						
ि Ignore X SJunk ≠ Delete	Reply Reply Forward More *	Lenovo To Manager Team Email	Mava	Gategorize ▼ Categorize ▼ Follow Up ▼	Translate ▼ Select ▼	Zoom	
Delete	Respond	Quick Steps	Move	Tags 🕞	Editing	Zoom	~
sun 4/19/2015 6:13 AM unsub-gpqpqjltizpkje@jedstock.com							

~

unsub-gpqpqjltizpkje@jedstock.com No Items

To Greg Scott

Boost your reputation of excellent lover

http://insider.theaidcompany.ru/ Little help for total joy

Click File...Properties

Properties					
Settings	Security				
Importanc Sensitivity	Add digital signature to outgoing message				
Do not A <u>u</u> toArchive this item					
Tracking options					
 Request a <u>d</u>elivery receipt for this message Request a <u>read receipt for this message</u> 					
Delivery options					
💁 Have replies	; sent to				
Expires a	fter None 👻 12:00 AM 👻				
<u>C</u> ontacts					
Categories None None					
Internet <u>h</u> eaders Received: from <u>46.98.198.194 (46.98.198.194)</u> by MAIL2013.infrasupport.local (10.10.10.12) with Microsoft SMTP Server id 15.0.913.22 via Frontend Transport; Sun, 19 Apr 2015 05:15:19 -0500 Received: from unknown (HELO localhost) (unsub- gpqpqjltizpkje@jedstock.com@137.174.225.63 by 46.98.198.194 with ESMTPA; Sun, 19 Apr 2015 14:17:45 +0300 From: < unsub-gpqpqjltizpkje@jedstock.com>					
	Close				

Look at the email header

Where did it really come from?

🎦 Yoast Google Analytics: D. 🗙 🗡 📧 46.98.198.194 WHOIS reg 🗴		
← → C 🗋 www.networksolutions.com/whois/res	sults.jsp?ip=46.98.198.194	* =
	🛿 VMware KB: Upgrad 🧭 Exchange Database 🍈 An evolution of Blac 🌃 www.sans.org/readi 🚾 Lenovo Solutions Ce 민 Ustream — The lead 🗋 New Tab	>>
501011	Call Now: 1-888-642-0221	*
	Cail Now. 1-868-042-0221	_
All Products	(S > Domain Names Websites eCommerce Hosting & SSL Professional Email Online Marketing	
	Search Renew Transfer Features Private Registration Protect Forward	_
		_
WHOIS Re		_
WHOIS RE	Search Again	_
You Sear	rched for: 46,98,198,194	_
		_
46.98.198.194 Record Type: IP /	Address Search again here	_
	Search by either	_
	Domain Name e.g. networksolutions.com IP Address e.g. 205.178.187.13	_
NetRange:	46.0.0.0 - 46.255.255.255	_
CIDR: NetName :	46.0.0/8 46-RIPE	_
NetHandle: Parent:	NET-6-0-0-0-0 ()	_
NetType: OriginAS:	Allocated to RIPE NCC	_
Organization:	RIPE Network Coordination Centre (RIPE)	_
RegDate: Updated: Dece	2009-09-29 2009-09-30	_
Ref:	http://whois.arin.net/rest/net/NET-46-0-0-0	
OrgName: OrgId:	RIPE Network Coordination Centre RIPE	
Address: City:	P.O. Box 10096 Amsterdam	
StateProv: PostalCode:	1001EB	
Country: RegDate:		
Updated: Ref:	2013-07-29 http://whois.arin.net/rest/org/RIPE	
ReferralServer:	r: whois://whois.ripe.net:43	
OrgTechHandle:		
OrgTechPhone:	RIPE NCC Operations +31 20 535 4444	
	hostmaster@ripe.net http://whois.arin.net/rest/poc/RNO29-ARIN	
	e: ABUSE3850-ARIN	
OrgAbusePhone:	Abuse Contact : +31205354444	
	: abuse@ripe.net http://whois.arin.net/rest/poc/ABUSE3850-ARIN	

🕒 Yoast Google Analytics: D. 🗙 📧 137.1	74.225.63 WHOIS re; ×
← → C 🗋 www.networksolution	pns.com/whois/results.jsp?ip=137.174.225.63
👯 Аррз 🚺 🕨 Громадське ONL 📑 Ya c	k Greg Scott is 🔤 VMware KB: Upgrad 🧭 Exchange Database խ An evolution of Blac 🌆 www.sans.org/readi 📴 Lenovo Solutions Ce 민 Ustream — The lead 🗋 New Tab »
	a WED.com company
	Call Now: 1-888-642-0221
	All Products > Domain Names Websites eCommerce Hosting & SSL Professional Email Online Marketing
	Search Renew Transfer Features Private Registration Protect Forward
	WHOIS Results
	Search Again
	You Searched for: 137.174.225.63
	137.174.225.63 Search again here
	Record Type: IP Address Search by either
	Domain Name e.g. networksolutions.com
	IP Address e.g. 205.178.187.13 NetRange: 137.174.0.0 - 137.174.255.255
	NetRange: 137,174,0.0/16 NetName: RIPE-ERX-137-174-0-0
	NetHandle: NET-137-174-0-0-1 Parent: NET137 (NET-137-0-0-0)
	NetType: Early Registrations, Transferred to RIPE NCC
	OriginAS: Organization: RIPE Network Coordination Centre (RIPE)
	RegDate: 2004-02-18 Updated: 2004-02-18
	Ref: http://whois.arin.net/rest/net/NET-137-174-0-0-1
	OrgName: RIPE Network Coordination Centre OrgId: RIPE
	Address: P.O. Box 10096
	City: Amsterdam StateProv:
	PostalCode: 1001EB Country: NL
	RegDate:
	Updated: 2013-07-29 Ref: http://whois.arin.net/rest/org/RIPE
	ReferralServer: whois://whois.ripe.net:43
	OrgAbuseHandle: ABUSE3850-ARIN OrgAbuseName: Abuse Contact
	OrgAbusePhone: +31205354444
	OrgAbuseEmail: abuse@ripe.net OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE3850-ARIN
	OrgTechHandle: RN029-ARIN
	OrgTechName: RIPE NCC Operations OrgTechPhone: +31 20 535 4444
	OrgTechEmail: hostmaster@ripe.net OrgTechRef: http://whois.arin.net/rest/poc/RN029-ARIN

Buy your copy today!

Bullseye Breach

ANATOMY OF AN ELECTRONIC BREAK-IN



Greg Scott – <u>gregscott@infrasupport.com</u> Twitter: DGregScott 1 (651) 260-1051

Warning: Don't start reading until a Friday because you won't be able to put it down.

This gives you the weekend to recover from jet-lag after reading all night.

http://www.bullseyebreach.com