RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

27 September 2017

TLP GREEN: Limited disclosure, restricted to the community. Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share **TLP GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP GREEN** information may not be released outside of the community.

CASE STUDY: PREPARATION FOR A WIRE FRAUD CAMPAIGN

IN BRIEF: In recent weeks, this author has received email messages of a suspicious nature. When shared with others in a meeting regarding email social engineering leading to wire fraud and BEC, Commercial Facilities Sector members were able to confirm that the messages are known to be part of the reconnaissance stage of the cyber kill chain. In fact, regional FBI offices have made private sector partners aware of such tactics and ask that such messages be shared with sector partners and reported to law enforcement. It should be noted that the messages did not solicit sensitive information nor were there any malicious links or attachments.

KEY TAKEAWAYS & RECOMMENDATIONS:

- This report includes sample messages and details that might raise suspicion for the recipient.
- Instructions for reporting such social engineering attempts to law enforcement will be included.
- The suspicious messages have already been shared with RE-ISAC members directly through the #incident_sharing channel on the RE-ISAC slack workspace.
- The details of the message have also been reported as possible fraud and abuse to the providers of the email services from which the messages originate.
- Details for protecting a business's identity and reputation from criminal impersonation and from BEC and wire fraud schemes are also included.

Between October 2013 and December 2016:
Domestic and international incidents: 40,203
Domestic and international exposed dollar loss: $5,302,890,448
The following BEC/EAC statistics were reported in victim complaints to the IC3 from October 2013 to December 2016:
Total U.S. victims: 22,292
Total U.S. exposed dollar loss: $1,594,503,669
Total non-U.S. victims: 2,053
Total non-U.S. exposed dollar loss: $626,915,475

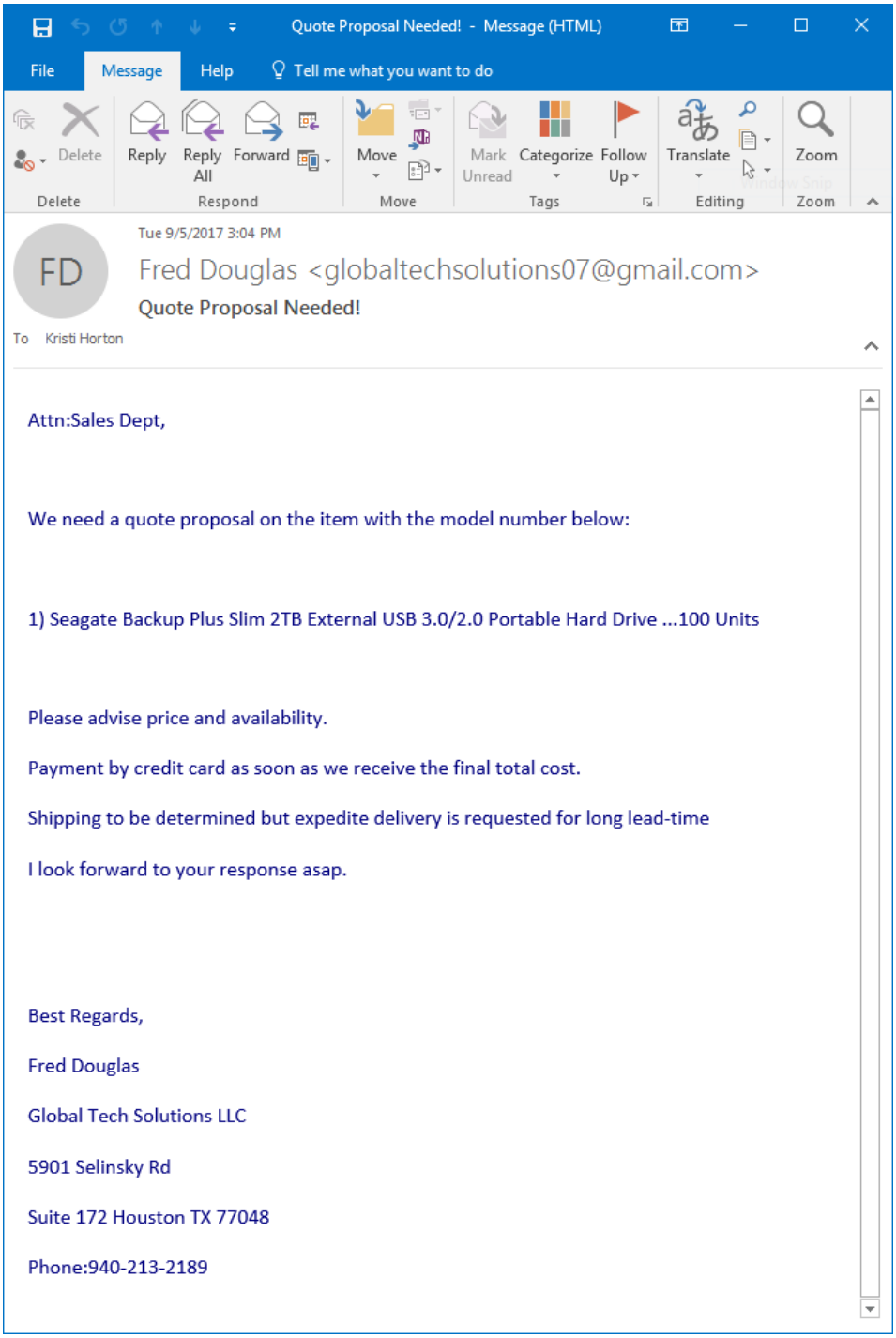
Source: FBI Alert Number I-050417-PSA

BACKGROUND. Over the last few months this author received messages claiming to be from legitimate businesses, but asking for quotes products and services the recipient organization does not provide. While the items listed might be consistent with work in the area of cybersecurity or digital forensics, the receiving organization does not normally just sell hard drives or external media, or other items listed in the requests. Upon further inspection of the emails, many (though not all) were directed to a contact email address listed on the business website. The others were addressed directly to the recipient's email address. In most cases the reply-to email address was a gmail account as opposed to an email address with a business domain name. The rest of the messages listed the gmail account as the "From" address. In each case, the messages listed a different email address and business name.

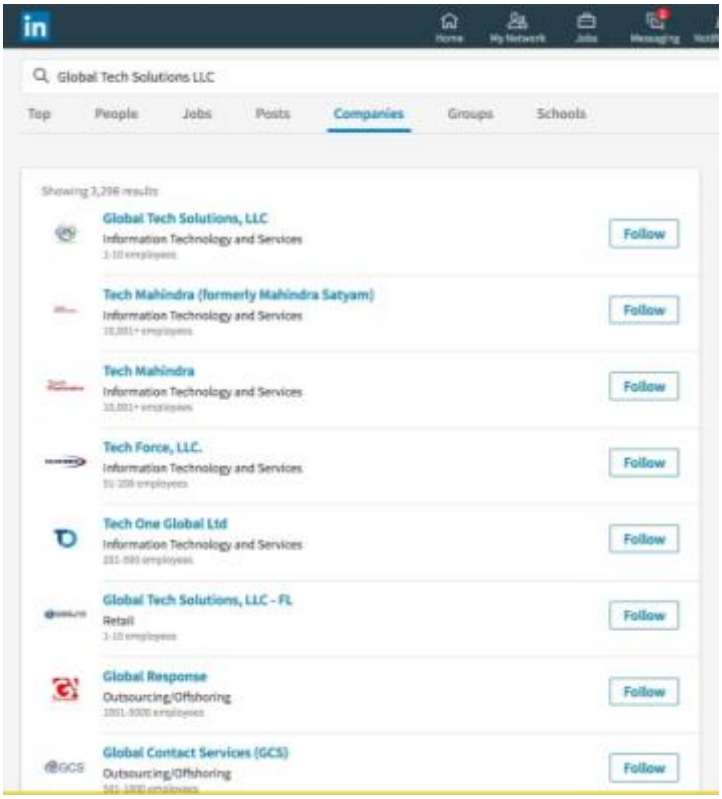
Because the emails complied with SPF and DKIM standards for messages coming from the originating domain, they did not immediately trigger any suspicion and were delivered to the inbox as opposed to spam or junk mail folders. The

messages would have been easy to dismiss as sloppy acquisition procedures on the part of another business entity. It was only the awareness of business email compromise and wire transfer schemes that caused this author to retain the information and document the events as suspicious as well as to seek counsel from peers in the RE-ISAC and law enforcement partners. The confirmation of similar events to gather information from legitimate businesses for the purpose of impersonating them or copying their proposal or invoicing documents caused this author to further research the specific characteristics of the suspicious messages.

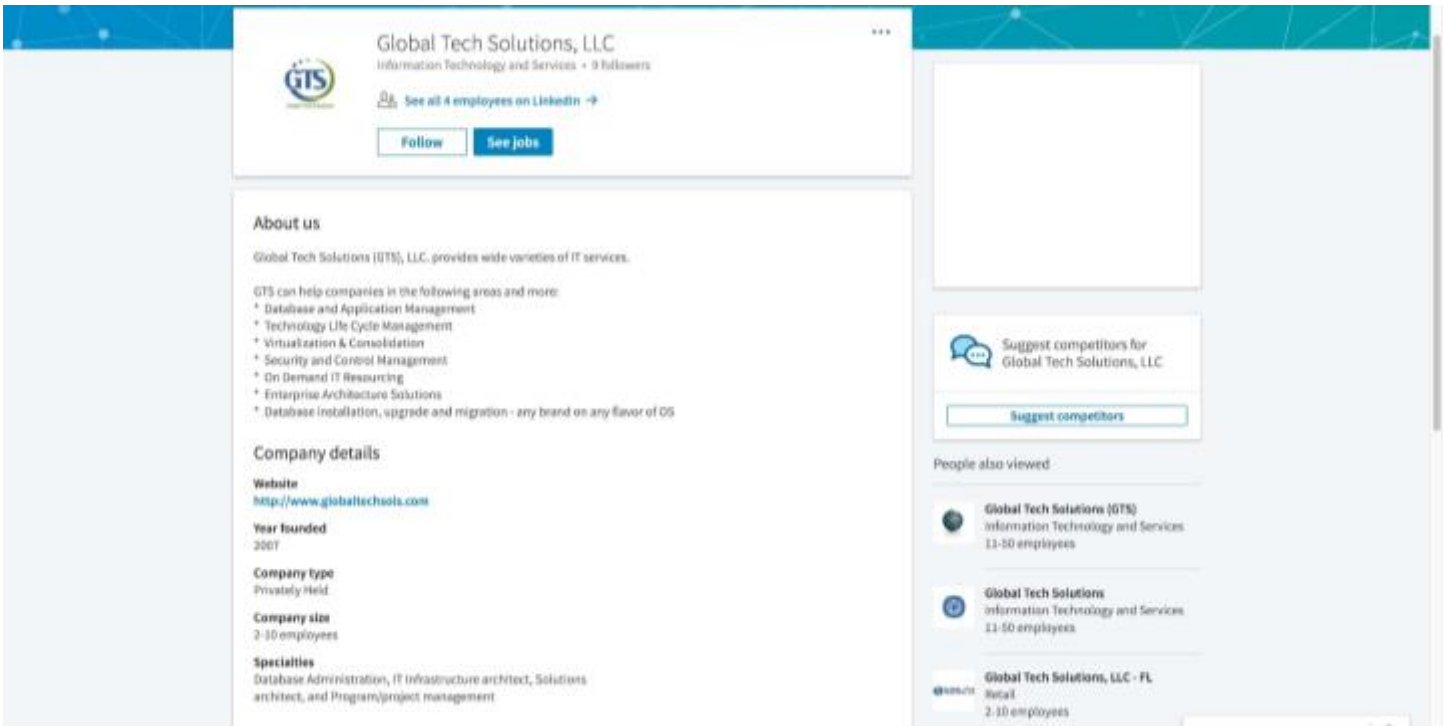
ANALYSIS. Sample message:

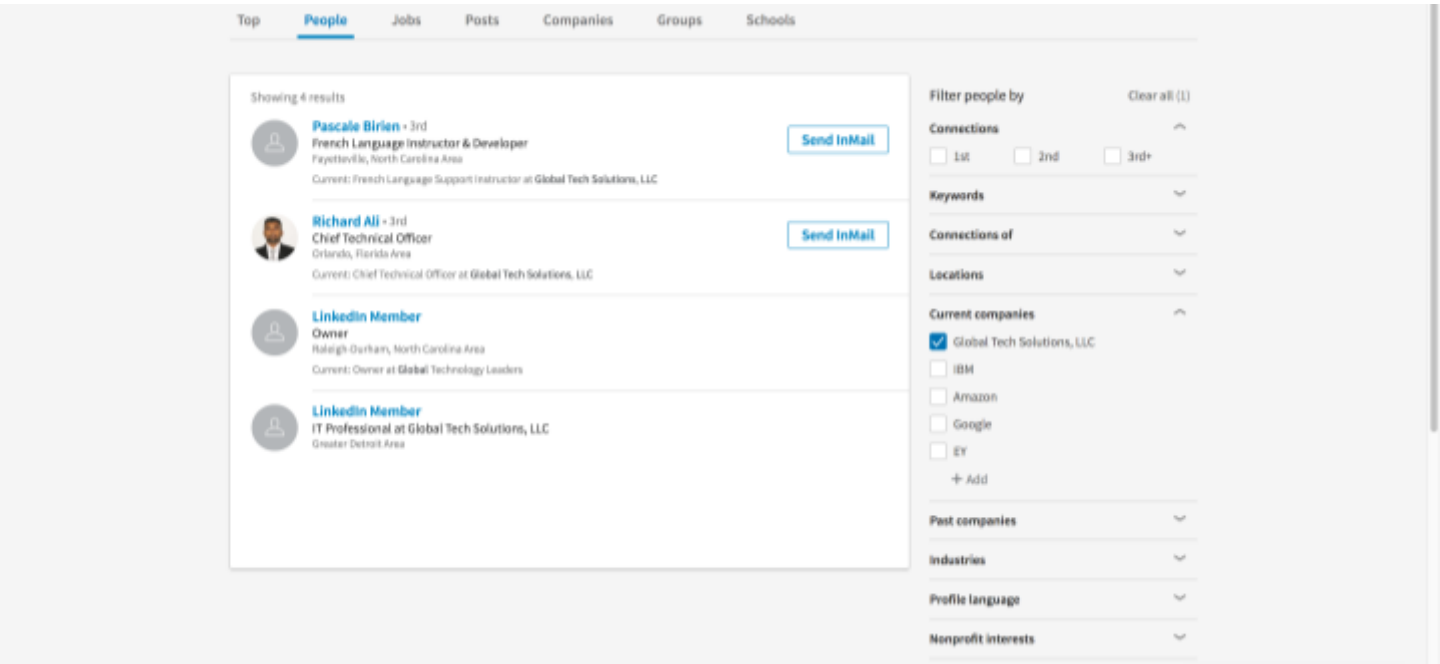


Because the email address seemed inconsistent with a legitimate business, this author conducted some research to better vet the purported potential client:



The first result in a search of companies on LinkedIn lists a Global Tech Solutions, LLC:





None of the people associated with this organization listed a location of Houston, TX, nor were any of them named Fred Douglas.

> ***Disclaimer**: finding an organization or purported employee on LinkedIn does not constitute an official record nor does it verify legitimacy. LinkedIn does not verify employment records, identities, or business information for LinkedIn accounts.*

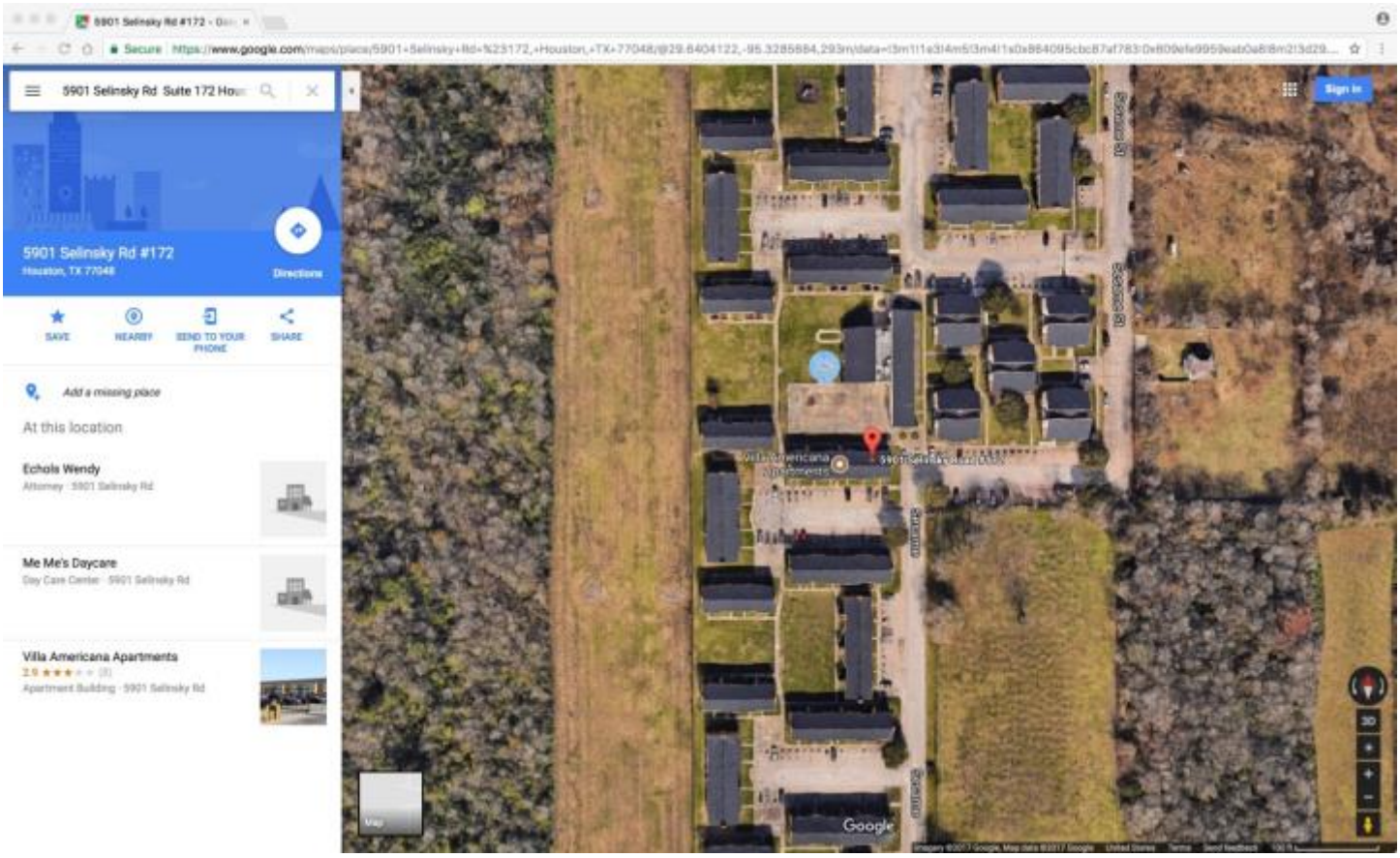
A second organization had a similar name, but listed FL in its LinkedIn title. Again, no people associated with that organization were named Fred Douglas nor were any people or addresses located in Houston, TX.

A visit to the websites of the organizations named Global Tech Solutions or similar also failed to reveal any further evidence of a location or employees in Houston, TX. The website for the first organization: globaltechsols.com, listed no physical address. No company owners or managers were identified and the only way to contact the organization was through a web form where the visitor's information was collected.

The website listed for the second possible result on LinkedIn, appeared to be unavailable. This author visited the sites of other search results from linked in. While the businesses appeared to be legitimate, no relationship was found with a Fred Douglas and none listed any locations in Houston, TX.

A search for any persons named "Fred Douglas" or similar names on LinkedIn did not list a Fred Douglas, rather a Frederick Douglas, but no one with a relationship to a Global Tech solutions company.

A search for the address in the email message on Google maps showed the building corresponding to the address. The address appears to be an apartment building also hosting a law office and day care, but no business called Global Tech Solutions was listed on the map.



In the absence of verifiable business entities or people mentioned in the email message, one could research business registrations with each state's regulatory commission or corporation commission or with the IRS. In this case, the business recipient does not sell the requested items. One further immediate examination of the email header information could yield further information. The data from the email header follows. Some notable fields are highlighted in yellow:

Return-Path: <n4edp_o4m5k@eteamz03w.email.active.com>

Received: from eteamz03w.email.active.com (eteamz03w.email.active.com [74.120.126.42])

by inbound-smtp.us-east-1.amazonaws.com with SMTP id c5darcmvs7g08fl1moj8euai27o94jn8sr3laqo1

for khorton@horton-innovations.com;

Tue, 05 Sep 2017 19:03:33 +0000 (UTC)

Received-SPF: pass (spfCheck: domain of eteamz03w.email.active.com designates 74.120.126.42 as permitted sender) client-ip=74.120.126.42; envelope-from=n4edp_o4m5k@eteamz03w.email.active.com; helo=eteamz03w.email.active.com;

Authentication-Results: amazonses.com;

spf=pass (spfCheck: domain of eteamz03w.email.active.com designates 74.120.126.42 as permitted sender) client-ip=74.120.126.42; envelope-from=n4edp_o4m5k@eteamz03w.email.active.com; helo=eteamz03w.email.active.com;

X-SES-RECEIPT:
AEFBQUFBQUFBQUFFbk9xU1BzR1pNeXk2UUx2WlZIMlVvU2k3bElUSE43QzBZekR0cVRBU1hmc2pXQmJ1VmdWaC9qSU40WlBhNVJnenowM3FQalovQkkvcC91YjFDdDdOQ1B2RnIrVFd3cmoxQnNWRGVlVWdBcHNWdGpmcG5BaUUvYncvNno4TEwxUVQ5eCtvcFcxc1FEQlRleTB3bEhJQXVZQTloVGwweHY1WVFZNkp6VGZWMWhMT2k0bjNTNUV4eEVSeUFEUkVodE9tWEJ6WUYxYkRZSGpxS0c5WTUzRDdMc0RIOWNzS2FpVDJNQi9YMGt4aHFJUVAzL2xXaGtBMnNNakx1WWNkajJHdmRQRUE1SStPNWRWR2hZbERGQ0tVc0JvMCtPTDFMMVpKeW0xMENSdjQva0E9PQ==

X-SES-DKIM-SIGNATURE: a=rsa-sha256; q=dns/txt; b=M3QyYn2Qy16YOHEvdOjRz6U32DNYDyvqHDdghDERq+MjFfSogOdsfmyGQ3GOKgReWnsF2mWy+/qAfHMzqnEQOL1HQXBfTURjWTzFJMR0uv2F4eN0ANqwY4iiLWR7KxYMXlKQTlks84S6hKv/DPFMCfJkb+t2c9fuG3zNk1CXBMk=; c=relaxed/simple; s=224i4yxa5dv7c2xz3womw6peuasteono; d=amazonses.com; t=1504638214; v=1; bh=35Fky2UEjoYLceOI7pf2gRf2gj2H5m7I//1c8u0YuJw=; h=From:To:Cc:Bcc:Subject:Date:Message-ID:MIME-Version:Content-Type:X-SES-RECEIPT;

Return-Path: <n4edp_o4m5k@eteamz03w.email.active.com>

Received: from [10.119.162.85] ([10.119.162.85:59003])

by epcl1mta02 (envelope-from <n4edp_o4m5k@eteamz03w.email.active.com>)

(ecelerity 3.6.3.44158 r(Platform:3.6.3.2)) with REST

id CF/96-15213-705FEA95; Tue, 05 Sep 2017 12:03:35 -0700

Date: Tue, 05 Sep 2017 12:03:35 -0700

Message-ID: <CF.96.15213.705FEA95@epcl1mta02>

MIME-Version: 1.0

From: "=?UTF-8?Q?Fred_Douglas?=" <globaltechsolutions07@gmail.com>

To: khorton@horton-innovations.com

List-Unsubscribe: <mailto:n4edp_o4m5k@eteamz03w.email.active.com?subject=remove>Subject: =?UTF-8?Q?Quote_Proposal_Needed!?=

The first notable item in the email header is the SPF check. Though a gmail account is used as the reply-to email address, the email message comes from the domain of eteamz03w.email.active.com the sending host is authorized by that domain to send email originating from that domain. This might mean that the domain has not been impersonated. While several facts regarding this message are suspicious, none of them alone (or even all of them taken together) constitute malicious activity or even criminal activity. The absence of verifiable business details regarding the purported sender or purported business remains suspicious. The recipient in this case, remains concerned that any activity confirming receipt of the message or any response to the message, will result in the impersonation of the business entity in criminal wire fraud or Business email compromise attempts against others.

Neither the email address, the sending IP addresses nor other data points in the message were listed as malicious in public registries of malicious indicators of compromise or other suspicious activity. The recipient needed more information, context and advice from peers. Information sharing and collaboration with sector peers and law enforcement partners revealed that these types of email messages might be the reconnaissance stage of business email compromise (BEC) or wire fraud campaigns. One tactic used in those campaigns is to impersonate legitimate businesses, send invoices in the name of the legitimate business, and direct funds to be paid to fraudsters. There are a few actions businesses can take to protect their reputation in these circumstances.

First**, implement SPF, DKIM, and DMARC policies regarding email sent from business domains**. Second, **purchase domains which may be similar to the business name**. If they cannot be purchased, monitor the registration of new domains that might impersonate your organization. Examples might be domains that substitute the number 0 for the letter o or the number 1 for the letter L. Alternatively, additional characters at the end of a domain which otherwise appears identical to the business domain. One more sophisticated approach may include the use of watermarks on images bearing company logos or documents that contain company information. More recent tactics can allow an organization to track the use of certain proprietary content across the Internet.

When receiving messages requesting information or emails requesting payments, **scrutinize messages from new customers or suppliers**. **Verify the source**. Ensure messages from recognized customers or suppliers actually came from the people known to your organization as opposed to an imposter. Verify any changes to payment arrangements in person or via a secondary communication channel such as a voice phone call.

Share information about fraud attempts and suspicious messages with other organizations in the Sector, and with other trusted sharing communities, if able.

IN ALL CASES, **report suspicious messages to law enforcement partners** (RE-ISAC can assist):

- FBI IC3: www.ic3.gov
- USSS Financial Crimes Task Force
- State Police Fraud investigation task forces

When requested to submit payments, follow ALL processes and procedures for wire transfers, checks, or card payments. Verify requests from company executives. Some firms have implemented an internal passphrase or codewords to be used to verify internal requests to make payments.