CITRA
الهيئة العامة للاتصالات و تقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Alert Date: 20 June 2020
Severity Level: ● Medium
Target segment: all

Security Alert

Description

There have been number of recent spoofing emails delivered to government entities within the state of Kuwait that look legitimate as if they have been sent by official email addresses related to MOH. The spoofing email have originated from a shared IP address provided by a hosting company located in Kazakhstan.

Threats

Spoofing is a tactic used in cyber-attacks in which malicious threat actors try to impersonate a domain in order to lure and deceive others. Threat actors attempt to lure users by emails from sources that look legitimate the reason for this is that they know that the chances of user interaction with messages are more likely.

Preventive Measures

- Provide Security awareness training programs to employees.
- Use organization email address based on assigned roles such as Public Relations, or customer relations.
- Deploy email security gateways which include malware protection, antispam and content filtering policies.
- Implement secure email authentication protocols (SPF, DMAC, DKIM).

Actions to take

- Be aware of this spoofing email campaigns.
- Review the image of the email header below.
- Kindly note that the Sending email domain IP is dynamic.

CITRA
الهيئة العامة للاتصالات وتقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Alert Date: 20 June 2020
Severity Level: ● Medium
Target segment: all

-----Original Message-----
Sent: Monday, June 15, 2020 12:58 PM
Subject: Message Notification

A message was processed that matched your filter 'Macro_Filter'
The headers from that message are:

From Email@moh.gov.kw Mon Jun 15 12:58:28 2020
X-IronPort-RCPT-TO:
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
d=pkz14.hoster.kz; s=hoster; h=Message-ID:Reply-To:Subject:To:From:Date:
Received: from [185.98.6.126] (helo=pkz14.hoster.kz)
by spamexpert1.hoster.kz with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
(Exim 4.92)
(envelope-from <Email@moh.gov.kw>)
id 1jkls2-000812-Mn; Mon, 15 Jun 2020 04:57:55 -0500
Received: from webmail.irtysh-hotel.kz (pkz14.hoster.kz [IPv6:::1])
by pkz14.hoster.kz (Postfix) with ESMTPSA id 851AB1D204A6;
Mon, 15 Jun 2020 15:57:07 +0600 (+06)
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="=_b647c012355a2bb7159ff17b7e0d877b"
Date: Mon, 15 Jun 2020 12:57:07 +0300
From: وزارة الصح
ة الكويت
<Email@moh.gov.kw>
To: undisclosed-recipients:;
Subject: (وزارة الص
حة الكويتية
التوزيع ال (
مجاني لمعدا
ك"ت الحماية
19 وفيد"
Reply-To: Email@moh.gov.kw
Mail-Reply-To: Email@moh.gov.kw
Message-ID: <Email@moh.gov.kw>
X-Sender: Email@moh.gov.kw
User-Agent: Roundcube Webmail/1.3.10
X-PPP-Message-ID: <Email@pkz14.hoster.kz>
X-PPP-Vhost: irtysh-hotel.kz
X-Originating-IP: 185.98.6.126
X-SpamExperts-Domain: pkz14.hoster.kz
X-SpamExperts-Username: 185.98.6.126
Authentication-Results: hoster.kz; auth=pass smtp.auth=185.98.6.126@pkz14.hoster.kz
X-SpamExperts-Outgoing-Class: ham
X-SpamExperts-Outgoing-Evidence: Combined (0.15)
X-Recommended-Action: accept
X-Report-Abuse-To: spam@spamexpert1.hoster.kz