Alla Dott.ssa Gemma Miliani,
Sostituto Procuratore, presso la
Procura della Repubblica di Perugia

E al: Dott. Luigi De Ficchy,
Procuratore Capo, presso la
Procura della Repubblica di Perugia

PROC. 4071 / 2017 RGNR PERUGIA

TENTATO ATTACCO INFORMATICO GMAIL

GIOVEDÌ 5 LUGLIO 2018

Egregia Dott.ssa Miliani,

desidero sottoporre alla Sua attenzione un tentativo di attacco informatico che ho subito oggi 5 Luglio, sulla mia Gmail il quale, per quanto Le vado ad esporre, potrebbe essere collegato alla vicenda attualmente oggetto delle Sue indagini.

In particolare, stamattina, accedendo via web alla mia Gmail giulio.occhionero@gmail.com ho trovato un messaggio dal Carcere di Viterbo, ovvero dal suo indirizzo viterbo@maidiremail.it che appartiene al notorio circuito di posta elettronica delle carceri Italiane, gestito da Aruba.

Il messaggio veniva già individuato da Gmail come *potenzialmente malevolo* per mezzo dell'inserzione di un banner di *alert* in cima al messaggio stesso. Tuttavia, la cosa che mi ha insospettito è che l'oggetto del messaggio conteneva il nominativo di "*Diego Paloni*", detenuto con il quale effettivamente corrispondo, avendolo conosciuto quando ero alla 6° sezione del C.C. Regina Coeli.

Al contrario delle ordinarie email di Maidiremail, che in genere contengono l'email scansionato in *.pdf* da un foglio di carta scritto a mano, visto che i detenuti non hanno accesso diretto ai pc con la posta, questo conteneva un allegato *.doc*.

I vecchi file Word .doc si prestano maggiormente all'inserimento al loro interno di codici eseguibili (anche malevoli) dato che possono contenere macro; le quali altro non sono che codice eseguibile Visual Basic for Applications (VBA).

Ulteriore elemento che desta sospetto è il fatto, però, che tale email in arrivo, riportasse in basso la mia ultima email inviata effettivamente a Paloni. Pertanto, chi ha composto questa email ha dovuto alternativamente:

- ottenere accesso alla mailbox del Carcere di Viterbo e prelevare la mia precedente email,
- avere accesso alla mia mail Gmail.

Tenderei ad escludere la seconda ipotesi, poiché (nei limiti dell'errore umano) io controllo regolarmente gli accessi precedenti alla mia Gmail e non ho notato nulla di strano. Ho, pertanto, fatto una rapida analisi degli *headers* di questo messaggio malevolo, che Le allego, assieme a quelli di un precedente messaggio regolare sempre arrivatomi da Viterbo.

Noterà immediatamente che il messaggio malevolo è transitato per McLink e sembra riportare come IP di partenza questo 104.245.195.122 di TekLinks, Birmingham, Alabama, USA. Tuttavia, come già detto anche nel nostro procedimento, ricordo che gli *headers* in sessione *smtp* possono essere parzialmente manipolati.

In particolare, sembra anche manipolato, secondo mia rapida ricostruzione, l'IP 172.24.30.43 che appartiene alla sottoclasse degli indirizzi *privati*, i quali raramente vengono riportati (anche perché non avrebbero gran significato) negli *headers*; come si evidenzia dallo Whois:

https://www.whois.com/whois/172.24.30.43

Tuttavia, ciò che non può essere modificato è la traccia lasciata da tale sessione nei log di McLink che bisognerebbe, a questo punto, esaminare. Negli stessi *headers*, compare anche questo saddisabilivr@codess.com che non si comprende bene se sia lo username utilizzato per l'autenticazione o altro.

Resto a Sua disposizione per inviarle anche l'allegato Word, in una forma che mi vorrà indicare, tale da non innescare impropriamente meccanismi antivirus.

Con osservanza,

Giulio Occhionero

Headers Messaggio Infetto

Delivered-To: giulio.occhionero@gmail.com
Received: by 2002:a17:90a:ad0:0:0:0:0 with SMTP id r16-v6csp1421886pje;
Wed, 4 Jul 2018 20:52:05 -0700 (PDT)
X-Google-Smtp-Source: AAOMgpfxOSYty1lwEs48R+XcyPakvRq73HBvHmP2/I94imMzEAvKmgd2yTWw+hYggUtr67qUgUbh
X-Received: by 2002:a1c:d92:: with SMTP id 140-v6mr2784590wmn.32.1530762725026;
Wed, 04 Jul 2018 20:52:05 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1530762725; cv=none;
d=google.com; s=arc-20160816;
b=TCRSgaYdGLVPFO3HVQS1vkYtt4vze2SAZkHAf7scVyIBtn8itfEekrg11LuXbPH5Z5
5bZL0HM9AVuf5QEkahCUx8O3xM8A90ZEu0TrIjBN7p7Xe4d9CDFqOE7MLGmdd1JFxadb
AGEI5rj52mSBPqqZxTHQz0Hv7A4xOOyDrltAgF1MiB5NHMS2LAOGpyCda/cRolPMdjXx
4v5ulNMt8onovRk5l+rFnF+ALq3/LWsm068OX+AHk6YFHC01g8vcZQoD8kbLTiE8ezTY
D9Mj0b0KS09yTq+2TFrEPxCLEe18AvtnQvksugQlzTJf1zSqq15xlumUVWb1VAFqJoz3
YmRw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=mime-version:references:in-reply-to:message-id:subject:from:to:date
:arc-authentication-results;
bh=KbuI4c2JE3o5TZCchL+CpZDSxWhfdvr7d/qDjTdl7gQ=;
b=cPioQRVRhKcMOkElWMegVGhGnhGMAxBlq2EF3fN3yXu+/roX/DlXCExWMmTW+J3iT5
xS5Yuyn7CU+MuR4PvIMn2P+aVpPhaiTXZwK/qmVcg4Oa/gvA83vfPFpYChjjaDy6JPk1
9dWbP40c+z7UUuUG5U+Kyx3KnP6fnW/RJlbvAukbCAMrHarwLQsILpMhe6smPcauGPaO
vBz36f+d7mqFIRdeaPg4oxRMjURyPI7p2d+YCiZoYPJxyyQNSYN/lgLUo3282uUouPmW
3tvk/Mqya6QG+xkSahvOeVgm9LRVSYHaYB3x8x3F6BCFJ7g8Hi1bdeWHwdgnUHIKFVlt
jRww==
ARC-Authentication-Results: i=1; mx.google.com;
spf=neutral (google.com: 77.43.14.229 is neither permitted nor denied by best guess record for domain of saddisabilivr@codess.com)
smtp.mailfrom=saddisabilivr@codess.com
Return-Path: <saddisabilivr@codess.com>
Received: from relaygw1-15.mclink.it (relaygw1-15.mclink.it. [77.43.14.229])
by mx.google.com with ESMTP id k7-v6si4077067wrf.130.2018.07.04.20.52.04
for <giulio.occhionero@gmail.com>;
Wed, 04 Jul 2018 20:52:04 -0700 (PDT)
Received-SPF: neutral (google.com: 77.43.14.229 is neither permitted nor denied by best guess record for domain of saddisabilivr@codess.com)
client-ip=77.43.14.229;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 77.43.14.229 is neither permitted nor denied by best guess record for domain of saddisabilivr@codess.com)
smtp.mailfrom=saddisabilivr@codess.com
Received: from [172.24.30.43] (HELO smtpoutgw3.mclink.it)
by relaygw1-15.mclink.it (CommuniGate Pro SMTP 6.0.2)
with ESMTP id 141117759 for giulio.occhionero@gmail.com; Thu, 05 Jul 2018 05:35:56 +0200
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result: A2CeBADokT1b/3rD9WjASgkCgRXAUow8
Received: from 104_245_195_122.teklinks.net (HELO localhost) ([104.245.195.122])
by smtpoutgw3.mclink.it with ESMTP; 05 Jul 2018 05:35:22 +0200
Date: Thu, 5 Jul 2018 03:35:19 +0000
To: giulio.occhionero@gmail.com
From: viterbo <viterbo@maidiremail.it>
Subject: Re: Re: PALONI DIEGO
Message-ID: <f9fa90e2b1cce81abdd96a0c0e1bba44@127.0.0.1>
X-Mailer: Outlook
In-Reply-To: <CAHYxXOqf5iUyZfri1XFiu4xCqaj02gQ3FhjsrkwnMC=SJxWOrA@mail.gmail.com>
References: <CAHYxXOqf5iUyZfri1XFiu4xCqaj02gQ3FhjsrkwnMC=SJxWOrA@mail.gmail.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="b1_f9fa90e2b1cce81abdd96a0c0e1bba44"

--b1_f9fa90e2b1cce81abdd96a0c0e1bba44
Content-Type: multipart/alternative; boundary="b2_f9fa90e2b1cce81abdd96a0c0e1bba44"

--b2_f9fa90e2b1cce81abdd96a0c0e1bba44
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

Buongiorno,

Vedi allegato e di confermare.

Grazie.

---
viterbo

Via delle Industrie, 11
20090 Vimodrone (MI)

Phone =C2=A0+39 02 274394224
Fax =C2=A0 =C2=A0 =C2=A0+39 02 274394112
Mobile =C2=A0+39 349 8866213

Headers Messaggio Regolare

Delivered-To: giulio.occhionero@gmail.com
Received: by 2002:a17:90a:1a17:0:0:0:0 with SMTP id 23-v6csp3705446pjk;
Mon, 18 Jun 2018 01:03:31 -0700 (PDT)
X-Google-Smtp-Source: ADUXVKJ88qISvb2+4EsziJC5AgIk/poR0D4OL08XUbQb//MN9BPyLDNv7pKb/EycaURy8o8raOB2
X-Received: by 2002:a1c:f0f:: with SMTP id 15-v6mr7284300wmp.141.1529309010854;
Mon, 18 Jun 2018 01:03:30 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1529309010; cv=none;
d=google.com; s=arc-20160816;
b=ddHvD0fZfgY3A3SE7aOaAV5O7yAE+HSKRz/A4c3hkVequsq0+I014EcKj+xWNYBSWD
reyJS5bNhsvK/ACqOhQgKM/ZZ8mrTt5dgf42S2A4N9gN+TywZF6ZPwG32gne0ft0cEZf
2pChE1h9HkRO9A0GQswFwisBxZ0g+INxcTvzC4iX0fc/KY1YxasTTSShotFYX3FVt/Xm
Ah/1j9fCNJPLutv+hCxtEvYXHbN/RMZ74eLLmAth2gCf8+0drHV75+Z3NxuZa6Ij+hGJ
chCw2anrXJxgQli3hX7SzGxX0n2CB/o1yhGhEq12BFt91F8rrhUtjf/wvZEe9JarIkdy
nwSQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=dkim-signature:content-language:thread-index:mime-version
:message-id:date:subject:to:from:arc-authentication-results;
bh=PJaL0SIkAmBOZ2WB3ARG3k/1WvPRaHDuNG4PVM0I1Ao=;
b=SSmHRXMHDxpJBybYdJa1jqrg8o+LGA6L3cD3D5iCZ8b6hZ0cHTrbWwWdez25y5RzmD
VMQp2E3v1WKVboPeyqH1gfaWAS/tqVp1vZrTHzNv4SQSXUlCNjEdjcHbqJNwpvTlekrk
u1QqiyQLcWk1tKxZqzTx6rBPUZiTbRrOQH5mrP73QaEoaTXAJRLZ5Ufp7jfW0Di26sWm
osZQd97jVxkqwurTlaAnZriPPADQkkOFxMea+LOZJxOFI9zjlyEqEzh7+4HRbLcVxI1r
QwLvKWROctyEacVlvg8izEsQ+ALCmlip47jYwYKGywIDxLrl1Pj3PeSUGI6/qJB4dD//
dmcw==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@aruba.it header.s=a1 header.b=S648Oquc;
spf=pass (google.com: domain of viterbo@maidiremail.it designates 62.149.156.56 as permitted sender)
smtp.mailfrom=viterbo@maidiremail.it
Return-Path: <viterbo@maidiremail.it>
Received: from smtpcmd0756.aruba.it (smtpcmd0756.aruba.it. [62.149.156.56])
by mx.google.com with ESMTPS id f2-v6si13590857wra.156.2018.06.18.01.03.30
for <giulio.occhionero@gmail.com>
(version=TLS1 cipher=AES128-SHA bits=128/128);
Mon, 18 Jun 2018 01:03:30 -0700 (PDT)
Received-SPF: pass (google.com: domain of viterbo@maidiremail.it designates 62.149.156.56 as permitted sender) client-ip=62.149.156.56;
Authentication-Results: mx.google.com;
dkim=pass header.i=@aruba.it header.s=a1 header.b=S648Oquc;
spf=pass (google.com: domain of viterbo@maidiremail.it designates 62.149.156.56 as permitted sender)
smtp.mailfrom=viterbo@maidiremail.it
Received: from adminPC ([93.71.246.128]) by smtpcmd07.ad.aruba.it with bizsmtp id 083V1y00c2mwmcD0183WNN; Mon, 18 Jun 2018 10:03:30 +0200
From: <viterbo@maidiremail.it>
To: <giulio.occhionero@gmail.com>
Subject: PALONI DIEGO
Date: Mon, 18 Jun 2018 10:03:25 +0200
Message-ID: <003301d406da$d596e420$80c4ac60$@maidiremail.it>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_NextPart_000_0034_01D406EB.99202950"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AdQG2tIj2PepcKLjSyurI6Yztq8emg==
Content-Language: it
X-Antivirus: Avast (VPS 180618-0, 18/06/2018), Outbound message
X-Antivirus-Status: Clean
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=aruba.it; s=a1; t=1529309010;
bh=PJaL0SIkAmBOZ2WB3ARG3k/1WvPRaHDuNG4PVM0I1Ao=; h=From:To:Subject:Date:MIME-Version:Content-Type;
b=S648Oquc3/hg4LDJizVREe2/FZQiv22A6arISP4NsPAQf0C/86ZfHHVY2jx7IuRTj
Hy+DALO1k/bGlYvf/0pNVcPjcr4LeDNP0EFD/qd+rHFo8sT43DR45BHOJxmk2FbFV3
gc+tEQSVUvypFseBhCOlPAQpyRscyPn77jiDp8GDRev1LABS5s5px3JYAWv+UHjRfP
BoFgqxijt6SdeymqOWHBFRXIOjlxzx/eFz5EKiVypP4eSseQ8L6RwWqw0bosJh61mj
FC5dS24/FwW4nMj9QImodxSzYcrcCpzkWMtgn5dVHENjL6b77j+8JO5QoR+cesbdJv
yGzagTvTuUO9A==

------=_NextPart_000_0034_01D406EB.99202950
Content-Type: multipart/alternative; boundary="----=_NextPart_001_0035_01D406EB.99202950"

------=_NextPart_001_0035_01D406EB.99202950
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

PALONI DIEGO le ha inviato un messaggio che trova in allegato. Per

rispondere dovr=E0 specificare in oggetto NOME e COGNOME del destinatario.Questa email =E8 strettamente confidenziale, nel caso le sia pervenuta per errore la preghiamo di cancellarla ed informarci, ogni utilizzo non autorizzato =E8 perseguibile.

PALONI DIEGO has sent you a message, please find it attached. To reply put in the subject FIRST and LAST NAME of the recipient.This email is strictly confidential, if you are not the intended recipient you are hereby notified that any use of it is prohibited, please delete it and notify the sender.

Questa e-mail =E8 stata controllata per individuare virus con Avast antivir=
us.
https://www.avast.com/antivirus