At Dr. Gemma Miliani , Deputy Prosecutor, at the Public Prosecutor of Perugia

And to: Dr. Luigi De Ficchy , Chief prosecutor at the Public Prosecutor of Perugia

P ROC. 4071 / 2017 RGNR P ERUGIA

T ented TO TTACCO THE NFORMATICO G MAIL

THURSDAY 5 JULY 2018

Egregia Dr. Miliani,

I wish to bring to your attention an attempt of attack I suffered today July 5th, on my Gmail, which, as Le'm going to expose, may be connected to each other currently the subject of your inquiries.

In particular, this morning, by going to my web Gmail giulio.occhionero@gmail.com I found a message from prison in Viterbo, or by its address viterbo@maidiremail.it which belongs to the well-known e-mail loop of Italian prisons, run by Aruba.

The message was already identified by Gmail as *potentially malicious* by placing their banner *alert* on top of the message itself. However, the thing that made me suspicious is that the object of the message containing the name of " *Diego Paloni* "Inmate with whom actually correspond, having met him when I was in the 6th section of the CC Regina Coeli.

Unlike ordinary email Maidiremail, which typically contain the email scanned in. *pdf* from a sheet of paper written by hand, as the prisoners have no direct access to PCs by postal mail, it contained an attachment. *Doc.*

The old Word .doc files allow for more inclusion in them of executable code (even malicious) as they may contain macros; which are nothing more than executable code Visual Basic for Applications (VBA).

A further element that arouses suspicion is the fact, however, that this incoming email, riportasse down my last email sent actually Paloni. Therefore, those who composed this email had to either:

- get access to the prison mailbox of Viterbo and withdraw my previous email,
- have access to my mail Gmail.

I would tend to exclude the latter, since (in the limits of human error) I check regularly the previous access to my Gmail and did not notice anything **strange. I, therefore, did a quick analysis of *headers* this malicious message, which I enclose, together with those of a previous regular message always** arrivatomi from Viterbo.

You will notice immediately that the malicious message is passed through McLink and looks back as IP starting this 104,245,195,122 of TekLinks, Birmingham, Alabama, USA. However, as already said in our case, remember that ***headers* in session *smtp* They may be partially manipulated.**

In particular, it seems manipulated, according to my quick reconstruction, the IP address 172.24.30.43 that belongs to the subclass *private,* which they are rarely reported (because they would not have much meaning) in *headers;* as evidenced by the Whois:

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

However, what can not be changed is the trail left by that session in McLink log that should, at this point, to examine. in the same *headers,* Also see this saddisabilivr@coc It does not understand well if both the username used for authentication or other.

Rest at your disposal to also send the attached Word, in a form that will take me indicate, such as not improperly trigger antivirus mechanisms.

With best regards,

Giulio Occhionero

Infected Message Headers

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 + / + l94imMzEAvKmgd2yTWw hYggUtr67qUgUbh X-Received: by 2002 a1c:
d92 :: SMTP id with 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
5bZL0HM9AVuf5QEkahCUx8O3xM8A90ZEu0TrljBN7p7Xe4d9CDFqOE7MLGmdd1JFxadb
AGEl5rj52mSBPqqZxTHQz0Hv7A4xOOyDrltAgF1MiB5NHMS2LAOGpyCda / 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 >
[redacted]
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
IronPort X-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.c om> References: <
CAHYxXOqf5iUyZfri1XFiu4xCqaj02gQ3FhjsrkwnMC=SJxWOrA@mail.gmail.c om> 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

Good morning,

See attached and confirm.

Thank you.

---

viterbo

Via delle Industrie, 11 20090
Vimodrone (MI)

Phone = C2 = A0 + 39 02 274 394 224
Fax = C2 = A0 = C2 = A0 = A0 = C2 + 39 02 274 394 112 Mobile = C2
= A0 + 39 349 8866213

Message Headers Set

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 + 4EsziJC5Aglk / poR0D4OL08XUbQb // MN9BPyLDNv7pKb / EycaURy8o8raOB2 X-Received: by 2002 a1c:
f0f :: SMTP id with 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 l014EcKj + xWNYBSWD reyJS5bNhsvK /
ACqOhQgKM / ZZ8mrTt5dgf42S2A4N9gN + TywZF6ZPwG32gne0ft0cEZf 2pChE1h9HkRO9A0GQswFwisBxZ0g +
INxcTvzC4iX0fc / KY1YxasTTSShotFYX3FVt / Xm Ah / 1j9fCNJPLutv + hCxtEvYXHbN / RMZ74eLLmAth2gCf8
0drHV75 + + + Z3NxuZa6lj hgj chCw2anrXJxgQli3hX7SzGxX0n2CB / o1yhGhEq12BFt91F8rrhUtjf / wvZEe9Jarlkdy
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:
dates: subject: to: from: arc-authentication-results; bh =
PJaL0SIkAmBOZ2WB3ARG3k / 1WvPRaHDuNG4PVM0I1Ao =;
b = + SSmHRXMHDxpJBybYdJa1jqrg8o LGA6L3cD3D5iCZ8b6hZ0cHTrbWwWdez25y5RzmD
VMQp2E3v1WKVboPeyqH1gfaWAS / tqVp1vZrTHzNv4SQSXUlCNjEdjcHbqJNwpvTlekrk
u1QqiyQLcWk1tKxZqzTx6rBPUZiTbRrOQH5mrP73QaEoaTXAJRLZ5Ufp7jfW0Di26sWm
osZQd97jVxkqwurTlaAnZriPPADQkkOFxMea LOZJxOFI9zjlyEqEzh7 + + + 4HRbLcVxI1r
QwLvKWROctyEacVlvg8izEsQ ALCmlip47jYwYKGywIDxLrl1Pj3PeSUGl6 / 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 ESMTPS id with 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: AdQG2tlj2PepcKLjSyurI6Yztq8emg ==
Content-Language: en
X-Antivirus: Avast (VPS 180618-0, 06/18/2018), 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 / gc rHFo8sT43DR45BHOJxmk2FbFV3 qd + + +
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 has sent a message that is attached. For

answer = E0 will have to specify FULL NAME object destinatario.Questa email = E8 confidence, in the case has been received in error please delete it and inform us of any unauthorized use actionable = E8.

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.
