ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Αρ. Πρωτ: L16-0412-02V1

Προς: κα Αλεξάνδρα Χρ. Κονίδα
Προϊσταμένη Δ/νσης Πληροφορικής & Νέων Τεχνολογιών

Κοιν: Πρόεδρο της Βουλής των Ελλήνων
Αντιπρόεδροι της Βουλής των Ελλήνων
κα Κατερίνα Μάρκου, βουλ. Β' Θεσσ. (Το ΠΟΤΑΜΙ)

Αθήνα, 11/5/2016

Κυρία Κονίδα,

Σε συνέχεια της ηλεκτρονικής επικοινωνίας μας (10/5) και της προηγούμενης επιστολής μας (12/4) με Αρ. Πρωτ.: L16-0412-01V1, σας αποστέλλουμε περισσότερες λεπτομέρειες και τεχνικά στοιχεία για το εν λόγω περιστατικό, όπως μας ζητήσατε:

1. Η αρχική διαπίστωση της προέλευσης έγινε μέσω του online spam reporting tool στο Spamcop.net, το οποίο εκτελεί αυτοματοποιημένο back-tracing και συνήθως εντοπίζει σωστά το domain, μερικές φορές και το sender email address. Στη συγκεκριμένη περίπτωση ανέφερε ως προέλευση τη διεύθυνση: "gv@parliament.gr" (IP: 195.251.32.41).

2. Επειδή ως domain name αναφέρεται το παλαιότερο της Βουλής, αντί το επίσημο σημερινό "hellenicparliament.gr", έγινε έλεγχος ταυτοποίησης για να διαπιστώσουμε ότι είναι ακόμα ενεργό και δείχνει όντως στο επίσημο δίκτυο της Βουλής, όπως και ισχύει.

3. Στο εν λόγω διαφημιστικό μήνυμα, καθώς και στις βασικές πληροφορίες αποστολής, αναφέρεται κάποια επιχείριση εστίασης και η ηλεκτρονική διεύθυνση "info@thissioview.gr". Τα στοιχεία της επιχείρισης, η διεύθυνση και τα τηλέφωνα επικοινωνίας αναφέρονται λεπτομερώς στο επισυναπτόμενο διαφημιστικό υλικό ("Μενού") του αρχικού μηνύματος.

4. Με αντίστοιχη διαδικασία, έγινε ταυτοποίηση του domain προέλευσης, καθώς και του registrar με όνομα Dataqube Ltd ("dataqube.gr" - IP: 195.129.40.126). Στο αρχείο του κεντρικού GR-Hostmaster αναφέρονται όλα τα στοιχεία, ονόματα και

τηλέφωνα του καταχωρητή, που πρακτικά είναι ο διαχειριστής του domain name “thissioview.gr”

5. Για την επιβεβαίωση της αναφοράς του Spamcop.net, καθώς και όλων των παραπάνω domain names και διευθύνσεων IP, ελέγχθηκαν διεξοδικά όλα τα βήματα προώθησης και οι ενδιάμεσοι κόμβοι που αναφέρονται στο header του αρχικού μηνύματος. Διαπιστώθηκε ότι όντως συμπίπτουν, δηλαδή πράγματι το μήνυμα έφυγε από την εν λόγω αρχική IP (εντός του δικτύου της Βουλής), χρησιμοποιώντας πιθανότατα κάποια εφαρμογή τύπου webmail (Horde5).

6. Επιπλέον, αξίζει να παρατηρηθεί ότι ως source IP αναφέρεται σαφέστατα η 195.251.32.41 και καμία άλλη ενδιάμεση ή εικονική (σε αγκύλες) IP, όπως συμβαίνει όταν μεσολαβεί (μέσω NAT) κάποια τοπική ευρυζωνική οικιακή σύνδεση τύπου ADSL ή VDSL με μη στατική IP. Επίσης αναφέρεται ως ενδιάμεσος κόμβος και η IP 195.129.40.126 της εταιρίας Dataqube Ltd, όπως αναφέρθηκε παραπάνω.

7. Από τα timestamps στους ενδιάμεσους κόμβους φαίνεται πως η αναφερόμενη ώρα είναι αξιόπιστη (συμπίπτουν με διαφορά ελάχιστων λεπτών). Συνεπώς η ώρα αποστολής του αρχικού μηνύματος είναι: Παρασκευή 8 Απριλίου 2015 ώρα 11:10' (τοπική).

Παρακάτω ακολουθεί το πλήρες header του αρχικού μηνύματος, όπου φαίνονται ξεκάθαρα όλες οι παραπάνω πληροφορίες:

```
Received: from MX2.webserve.gr (172.16.8.114) by CAS01.webserve.gr
 (172.16.9.43) with Microsoft SMTP Server (TLS) id 8.3.245.1; Fri, 8 Apr 2016
 11:12:49 +0300
Received: from cloud01.dataqube.gr (95.129.40.126) by MX2.webserve.gr
 (172.16.8.114) with Microsoft SMTP Server (TLS) id 8.3.245.1; Fri, 8 Apr 2016
 11:12:30 +0300
Received: from cloud01.dataqube.gr (localhost [127.0.0.1])       by
 cloud01.dataqube.gr (Postfix) with ESMTPSA id 90F72642E6;       Fri,  8 Apr 2016
 11:10:07 +0300 (EEST)
Received: from 195.251.32.41 ([195.251.32.41]) by webmail.thissioview.gr
        (Horde Framework) with HTTP; Fri, 08 Apr 2016 08:10:07 +0000
From: "info@thissioview.gr" <info@thissioview.gr>
Disposition-Notification-To: "info@thissioview.gr" <info@thissioview.gr>
Date: Fri, 8 Apr 2016 11:10:07 +0300
Subject: RESTAURANT THISSIO VIEW-THE BEST ACROPOLIS VIEW-MENU 2016
Thread-Topic: RESTAURANT THISSIO VIEW-THE BEST ACROPOLIS VIEW-MENU 2016
Thread-Index: AdGRbnCD4HMW5ShIR8SdAWMSDDLnqg==
Message-ID:
 <20160408081007.Horde.XvSG_jW3NS3QK3EpD3pyprr@webmail.thissioview.gr>
Accept-Language: en-GB, en-US, el-GR
Content-Language: el-GR
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-AuthSource: MX2.webserve.gr
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SenderIdResult: Pass
X-MS-Exchange-Organization-PRD: thissioview.gr
X-MS-TNEF-Correlator:
received-spf: Pass (MX2.webserve.gr: domain of info@thissioview.gr
 designates 95.129.40.126 as permitted sender) receiver=MX2.webserve.gr;
 client-ip=95.129.40.126; helo=cloud01.dataqube.gr;
domainkey-signature: a=rsa-sha1;  q=dns; c=nofws;  s=default;
 d=thissioview.gr;
  b=m9Ni5WERIRMjQ5aQJ+gKRGyPo55Uy+HcJeBhrhFP6wvGvaZCwYcJsFaOtBuV7glz1Pi+8drYbh4p8P7LNxSlOEmTVL2ATjG
ohp+0C7OtYUHRGV4hKrpQSixHHw4ysKfv0G5MxHbWTUF/IQ3ZGEeFyb3YO6Jj/QzG6Ccl3gi9bK0=;
         h=Received:Date:Message-ID:From:To:Subject:Disposition-Notification-To:User-Agent:Content-
Type:MIME-Version:Content-Transfer-Encoding:X-PPP-Message-ID:X-PPP-Vhost;
user-agent: Horde Application Framework 5
x-ppp-message-id: <20160408081007.25002.968@cloud01.dataqube.gr>
x-ppp-vhost: thissioview.gr
Content-Type: multipart/mixed;
        boundary="_003_20160408081007HordeXvSGjW3NS3QK3EpD3pyprrwebmailthissio_"
MIME-Version: 1.0
```

Μαζί με την παρούσα επιστολή, αποστέλλουμε ηλεκτρονικά και όλα τα σχετικά αρχεία τεκμηρίωσης που αφορούν στα παραπάνω.

Ως τελικός αποδέκτης, από τη μεριά μας δεν έχουμε ούτε την τεχνική ούτε τη νομική δυνατότητα να αντλήσουμε περισσότερες πληροφορίες για το περιστατικό. Δεν είναι στην αρμοδιότητά μας, ούτε και επιθυμούμε, να εκθέσουμε επίσημη γνωμοδότηση ή να καταδείξουμε πιθανούς ενόχους. Θεωρούμε, όμως, ότι πρόκειται για μείζον ζήτημα που

πλήττει σοβαρότατα, όχι μόνο το κύρος της Βουλής, αλλά και την εμπιστοσύνη σε ότι αφορά την εφαρμοζόμενη Πολιτική Ασφάλειας (Security Policy) στο εσωτερικό της δίκτυο.

Συνεπώς, όπως έχουμε ήδη αναφέρει στην προηγούμενη επιστολή, επιφυλασσόμαστε να γνωστοποιήσουμε το συγκεκριμένο συμβάν σε αρμόδιους κρατικούς φορείς και ανεξάρτητες Αρχές, αλλά και σε όποιον μπορεί να συνδράμει για να εντοπιστούν οι υπεύθυνοι και να μην επαναληφθούν παρόμοια περιστατικά, που εκθέτουν το ελληνικό Κοινοβούλιο και προσβάλλουν τη νοημοσύνη των πολιτών.

Ελπίζουμε να έχουμε ήδη συνεισφέρει προς αυτή την κατεύθυνση. Για οποιαδήποτε επιπλέον πληροφορία ή τεχνική συνδρομή, φυσικά είμαστε στη διάθεσή σας.

ΥΓ: Η παρούσα επιστολή κοινοποιείται, εκτός από το Προεδρείο της Βουλής, και στην κυρία Κατερίνα Μάρκου, βουλευτή Β' Θεσσ/νίκης με το ΠΟΤΑΜΙ, η οποία εχθές (10/5) μας κοινοποίησε την αντίστοιχη επιστολή της σχετικά με το ίδιο θέμα.

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Ο Πρόεδρος	Ο Αντιπρόεδρος	Ο Γενικός Γραμματέας	Ο Ειδικός Γραμματέας	Η Ταμίας
Δημήτρης Κυριακός	Γιάννης Κιομουρτζής	Χάρης Γεωργίου	Φώτης Αλεξάκος	Λένα Καπετανάκη
proedros@epe.org.gr	antiproedros@epe.org.gr	gen_grammateas@epe.org.gr	eid_grammateas@epe.org.gr	tamias@epe.org.gr

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
Email: info@epe.org.gr – Τηλέφωνο/Fax: 211-7907675