



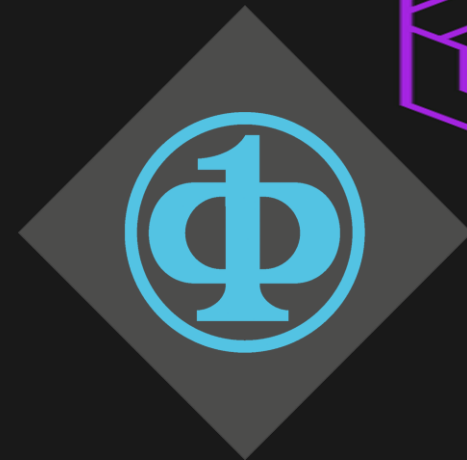
PHISHING ATTACKS: BEHIND THE SCREENS

POWERED BY IEEE NTU AS



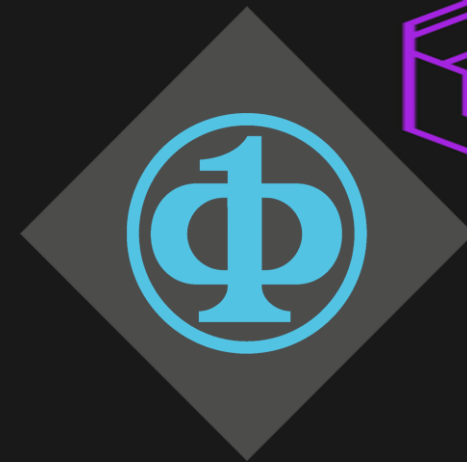
ETHICAL HACKING

COMPUTER SOCIETY CHAPTER





To Computer Society Chapter



cs.ntua@gmail.com



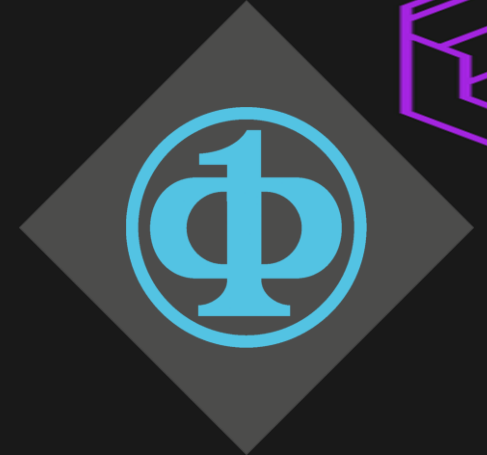
[@CS Chapter IEEE NTUA SB](#)



[@cs.ntua](#)



Η δράση του Ethical Hacking



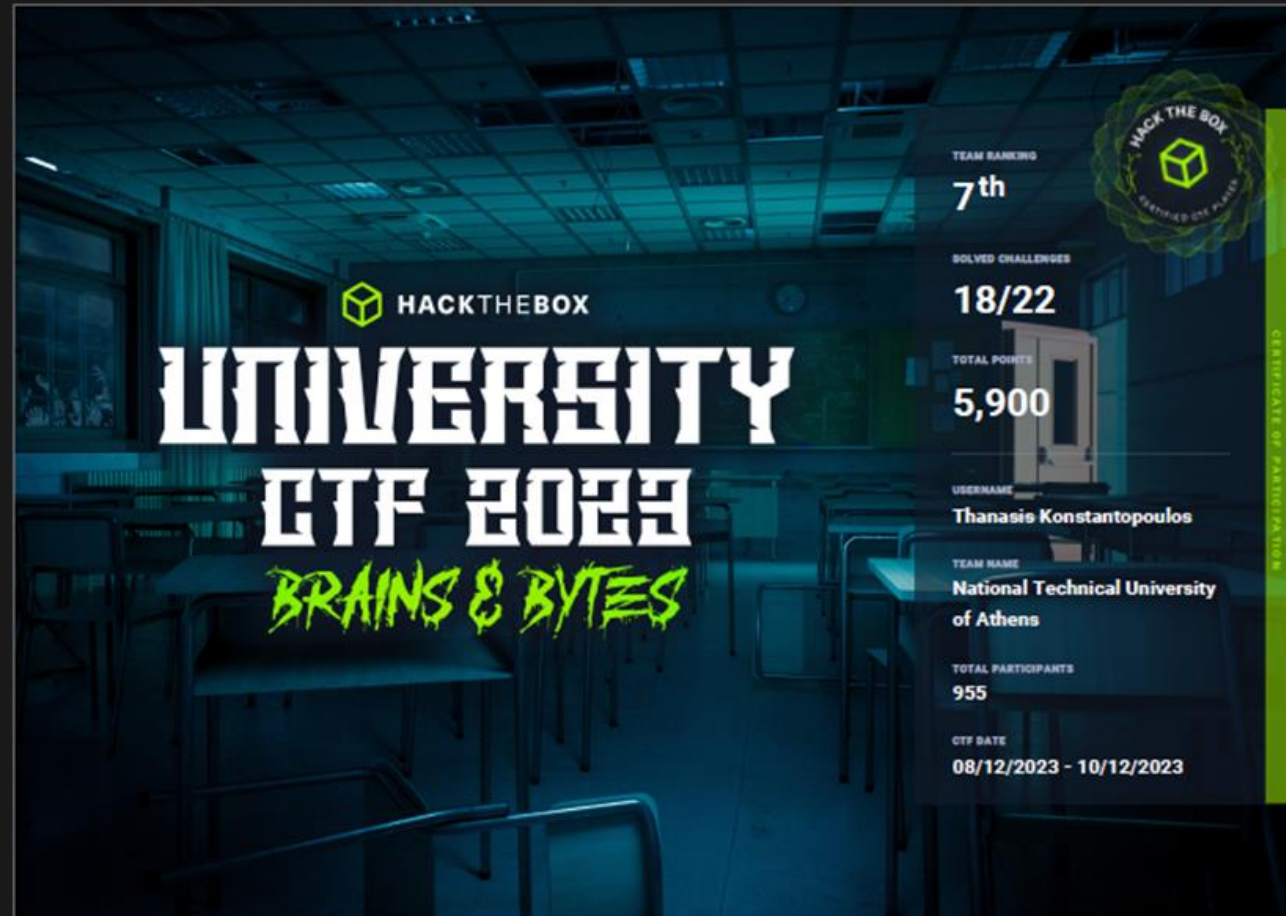
- ➔ Συμμετοχή σε αναγνωρισμένους, διεθνείς διαγωνισμούς CTF (Capture The Flag)
- ➔ Διεξαγωγή event (NTUA_H4CK 1.0, NTUA_H4CK 2.0)
- ➔ Training φοιτητών, εβδομαδιαίας βάσης, σχετικά με το CyberSecurity (Διαλέξεις, Παρουσιάσεις, mini-workshop, ctf on the spot)



HTB University CTF – Brains and Bytes



Online - December 2023
Final ranking: 7/955





26-27 NOV 2022

POWERED BY IEEE NTUA SB



NTUA_HACK

THE ETHICAL HACKING CHALLENGE

OUR SUPPORTERS



HACKTHEBOX



15-17 DEC 2023

POWERED BY IEEE NTUA SB



NTUA_HACK

THE ETHICAL HACKING CHALLENGE

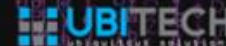
OUR SUPPORTERS



OBRELA



accenture





Τριημερίδα NTUA_H4CK 2.0



Τα παρακάτω στατιστικά προέκυψαν μετά απο έρευνα σε 500 security professionals.

94% των οργανισμών έπεσαν θύματα επιθέσεων phishing και το 96% από αυτούς επηρεάστηκαν αρνητικά από αυτές.

Σε 74% των οργανισμών, οι εργαζόμενοι που εμπλέκονταν τιμωρήθηκαν, απολύθηκαν ή αποχώρησαν εθελοντικά.

Το 58% υπέστησαν επιθέσεις λογαριασμών.

Το 79% αυτών των επιθέσεων ξεκίνησε με ένα phishing email και στο 83% είχε παραβιαστεί το (MFA) για να επιτευχθεί η επίθεση.

Το 61% των Cybersecurity leaders λένε ότι η χρήση chatbots στο phishing τους κρατάει ξύπνιους τη νύχτα.

Το 91% έχει ανησυχίες με τον Έλεγχο Ηλεκτρονικής Αλληλογραφίας (SEG) τους και το 90% με τους στατικούς κανόνες Προστασίας Δεδομένων στην Αναχώρηση (DLP).

Info: <https://www.egress.com/blog/phishing/phishing-statistics-round-up>

Data loss & exfiltration stats

Το 94% είχε περιστατικά που προκλήθηκαν από απώλεια και κλοπή δεδομένων, μια αύξηση 8% σε σχέση με τις περσινές επιθέσεις.

Το 91% των οργανισμών είχε αρνητικές επιπτώσεις.

Το 67% των εμπλεκόμενων άτομων επηρεάστηκαν.

Το 57% είχε χρηματοοικονομικές απώλειες σε κάποιο βαθμό.

Το 46% είδε τον τζίρο να μειώνεται λόγω αποχώρησης πελατών.

Το 40% είδε ζημιά στη φήμη της εταιρείας τους.

Λίγα λόγια

- Πρόκειται για επίθεση που στηρίζεται κυρίως σε **social engineering**
- Ο επιτιθέμενος προσπαθεί να εξαπατήσει τα άτομα που επιθυμεί ώστε να του αποκαλύψουν ευαίσθητες πληροφορίες
- Άλλες φορές πάλι, η εξαπάτηση έχει ως στόχο την εγκατάσταση κακόβουλου λογισμικού (malware) σε μηχανήματα των «θυμάτων»
- Σε κάθε περίπτωση, συνιστά αρκετά επικίνδυνη μορφή επίθεσης



Μα εγώ ξέρω... δεν την πατάω



- Αυτό θα ήταν πολύ ωραίο αλλά φιλαράκια μου δυστυχώς...
- Πρόκειται για τη συχνότερη μορφή κυβερνοεγκλήματος με πάρα πολλά θύματα ετησίως

Ενδεικτικά:

- Το **83%** των επιχειρήσεων του Ηνωμένου Βασιλείου που αποτέλεσαν θύμα κυβερνοεπίθεσης το 2022, οφειλόταν σε phishing.
- Η Google μπλοκάρει περί των 100 εκατομμυρίων phishing emails καθημερινά
- Πιθανότατα και εσείς έχετε λάβει κάποια στιγμή «ύποπτα» emails ή SMS

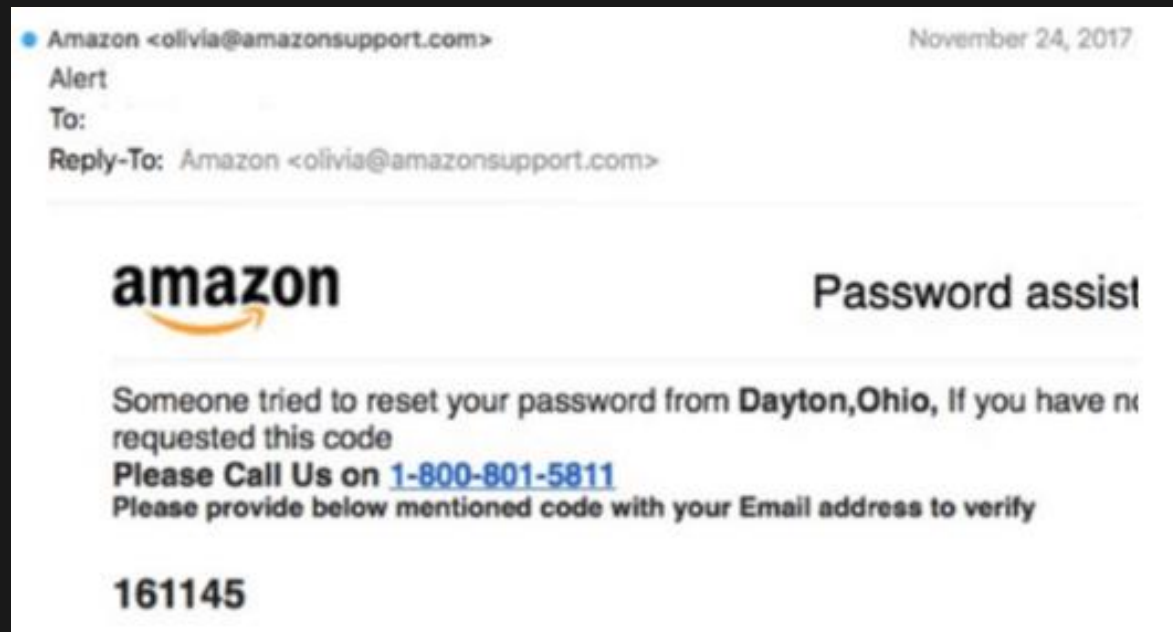
Γιατί κυριαρχεί το Phishing

- Εύκολη μέθοδος επίθεσης (κυρίως μέσω **emails**) χωρίς ιδιαίτερους περιορισμούς και έξοδα
- Μπορεί να επηρεάσει την πλειοψηφία των χρηστών του διαδικτύου
- Κατά βάση, δεν απαιτεί ιδιαίτερες γνώσεις και δεξιότητες από τον επιτιθέμενο (αυτό δεν ισχύει για το κακόβουλο λογισμικό που συχνά περιέχουν οι επιθέσεις τύπου phishing)
- Έλλειψη επαρκούς ενημέρωσης και κατάρτισης των χρηστών του διαδικτύου ώστε να αναγνωρίζουν phishing attacks (αυτό ισχύει ακόμα και για νέους)

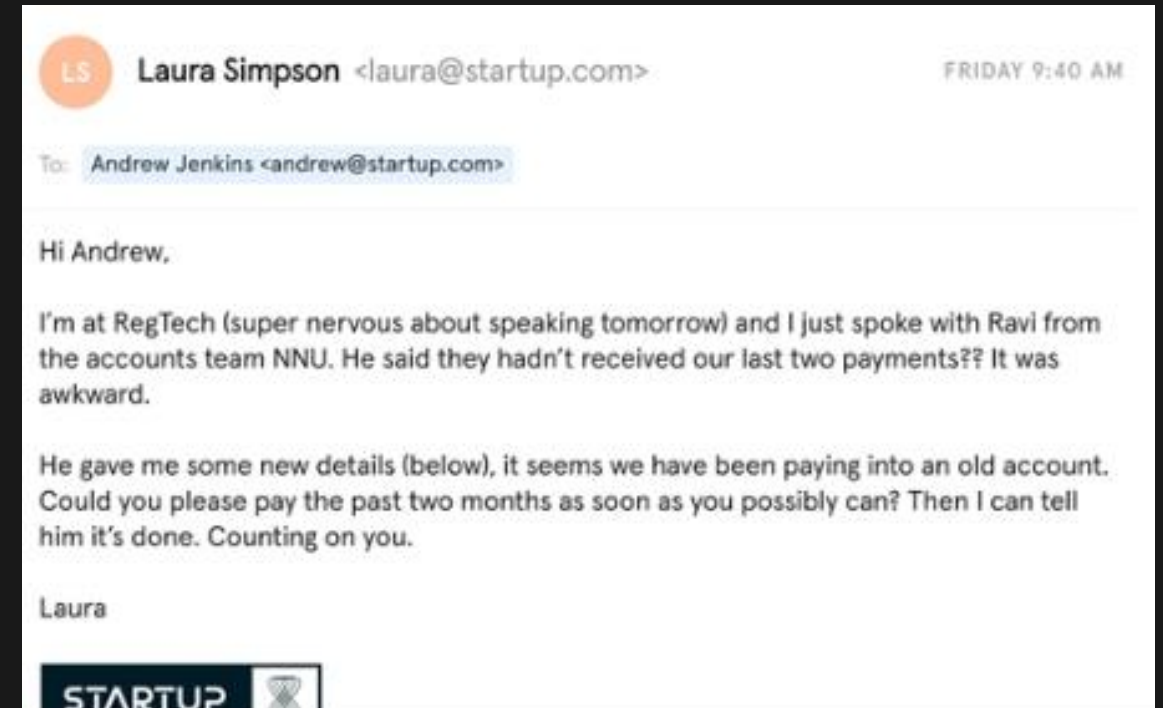
Τύποι phishing

- **Email phishing:** Συνιστά τη συχνότερη μορφή επίθεσης Phishing. Ο επιτιθέμενος αποστέλλει μαζικά emails από fake domain (περισσότερα στο demo που θα ακολουθήσει 😊).
- **Spear phishing:** Και πάλι πραγματοποιείται μέσω email, ωστόσο τώρα γίνεται στοχευμένα καθώς ο επιτιθέμενος γνωρίζει αρκετές πληροφορίες (όνομα, επάγγελμα κ.α.) για τον «στόχο» του.

Email Phishing example



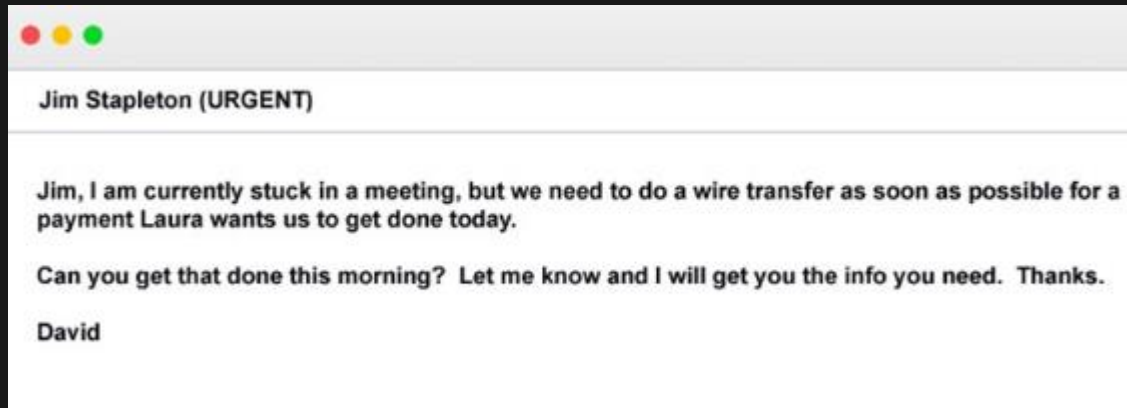
Spear Phishing example



Τύποι phishing

- **Whaling:** Πρόκειται για ακόμα πιο στοχευμένο τύπο επίθεσης κυρίως σε ανώτατα στελέχη μίας επιχείρησης (ξανά μέσω email)
- **Smishing:** Το ίδιο με το απλό email phishing, απλώς τώρα η αποστολή του μηνύματος γίνεται μέσω SMS (συχνά ο επιτιθέμενος υποδύεται κάποια τράπεζα)
- **Vishing:** Στη συγκεκριμένη μορφή, χρησιμοποιείται το τηλέφωνο (Voice phishing) ως το μέσο επικοινωνίας του attacker με το εκάστοτε «θύμα»

Whaling example



Smishing example

HSBC ALERT: Request for NEW payee MR D FRASER has been made on your account. If this was NOT done by you, visit: hs-internet-cancel-payees.com/login

Πώς αναγνωρίζουμε ένα phishing email

Όσο προσεκτικοί και αν είμαστε, σε μια μορφή στοχευμένου phishing πιθανότατα οι περισσότεροι δε θα συνειδητοποιούσαμε την απάτη.

Ωστόσο, τα περισσότερα phishing emails που θα λάβετε δεν αφορούν μόνο εσάς (main character syndrome), αλλά ανήκουν σε αυτό που λέμε καμπάνιες (**campaigns**).

Καμπάνια: Μια εκστρατεία phishing, δηλαδή emails που μοιάζουν μεταξύ τους είτε ως προς το περιεχόμενο, είτε χρησιμοποιούν παρόμοια υποδομή (domains, phishing sites). Τα emails στέλνονται σε πολλαπλούς παραλήπτες, με σκοπό να καταφέρουν να ξεγελάσουν το δυνατόν περισσότερους.

Τι μπορώ να κάνω ως χρήστης;

Να μάθεις να αναγνωρίζεις κάποια κοινά χαρακτηριστικά των phishing e-mails.

- Γραμματικά, συντακτικά και νοηματικά λάθη: Πολλές καμπάνιες οργανώνονται στο εξωτερικό. Οι επιτιθέμενοι (scammers) σκέφτονται ότι θα πείσουν περισσότερο κόσμο αν περάσουν το email από google translate πριν το αποστείλουν.



Τετ 25.02.2021 17:04

EuroBank-gr <masayo.t@[REDACTED].site>

Η πρόσβασή σας δεν είναι ενεργή!

To [REDACTED] gr



Αγαπητέ πελάτη

Έχουμε τοποθετήσει προσωρινά κλειδαριά στην κάρτα σας!

Οι διαδικτυακές πληρωμές και αναλήψεις μετρητών δεν μπορούν να γίνουν έως ότου επιλυθεί αυτό το ζήτημα. Επιβεβαιώστε την πρόσβασή σας εντός των επόμενων 48 ωρών.

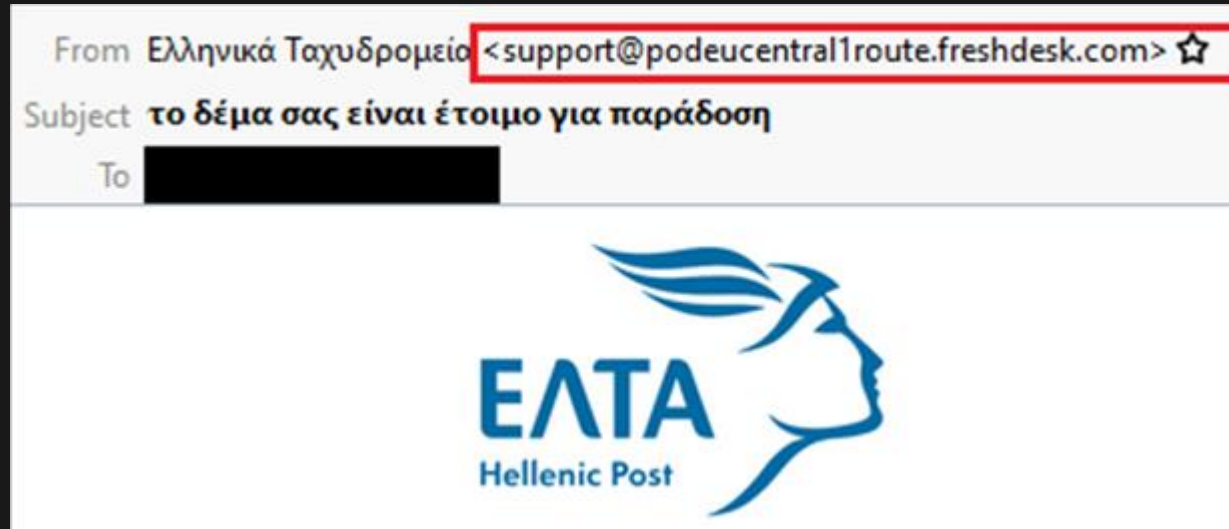
[Ενεργοποίηση τώρα](#)

Απαντήστε σε αυτό το e-mail εάν έχετε περαιτέρω απορίες ή θέλετε να επικοινωνήσετε μαζί μας.

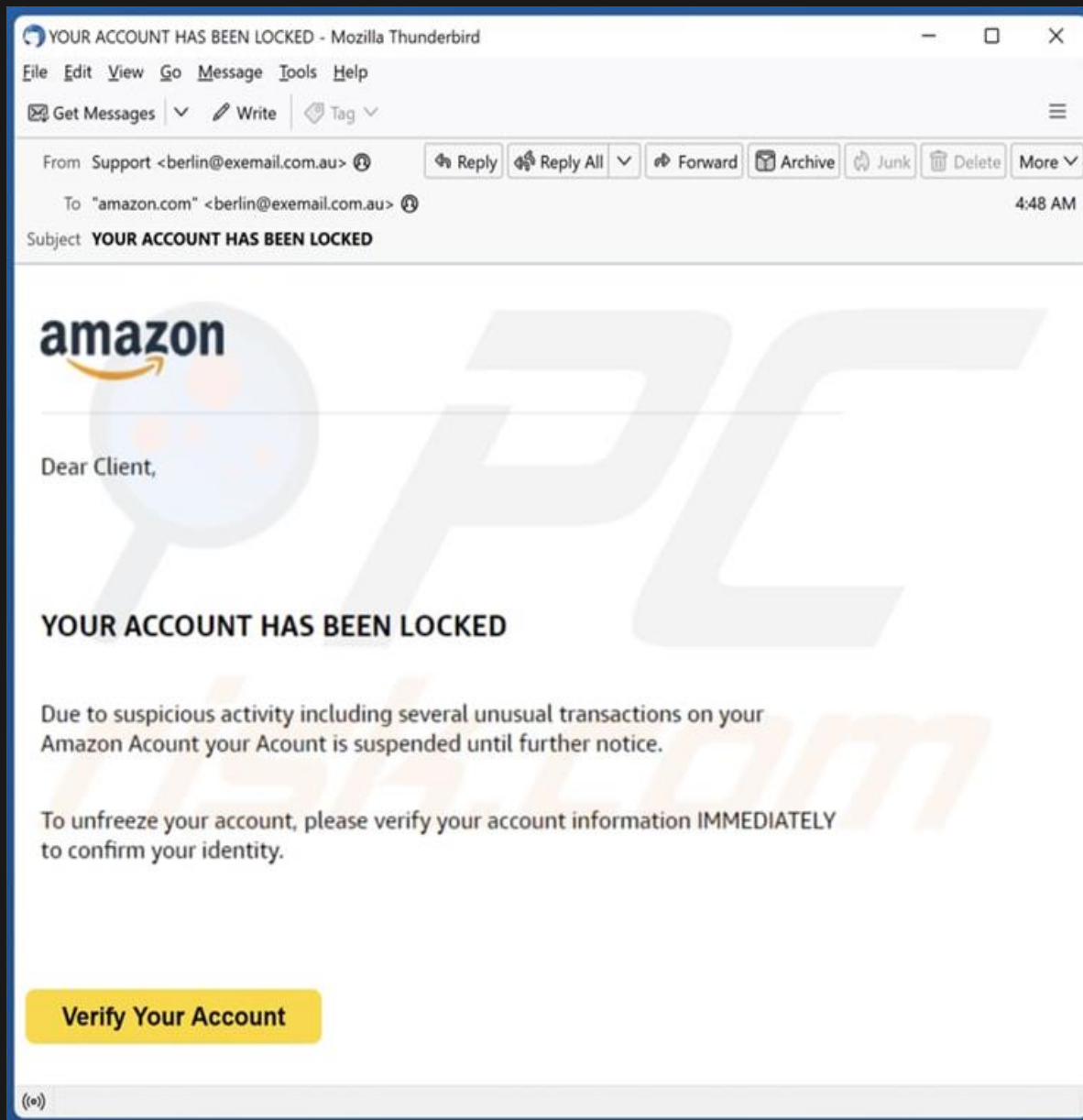
Θερμούς χαιρετισμούς,
EuroBank



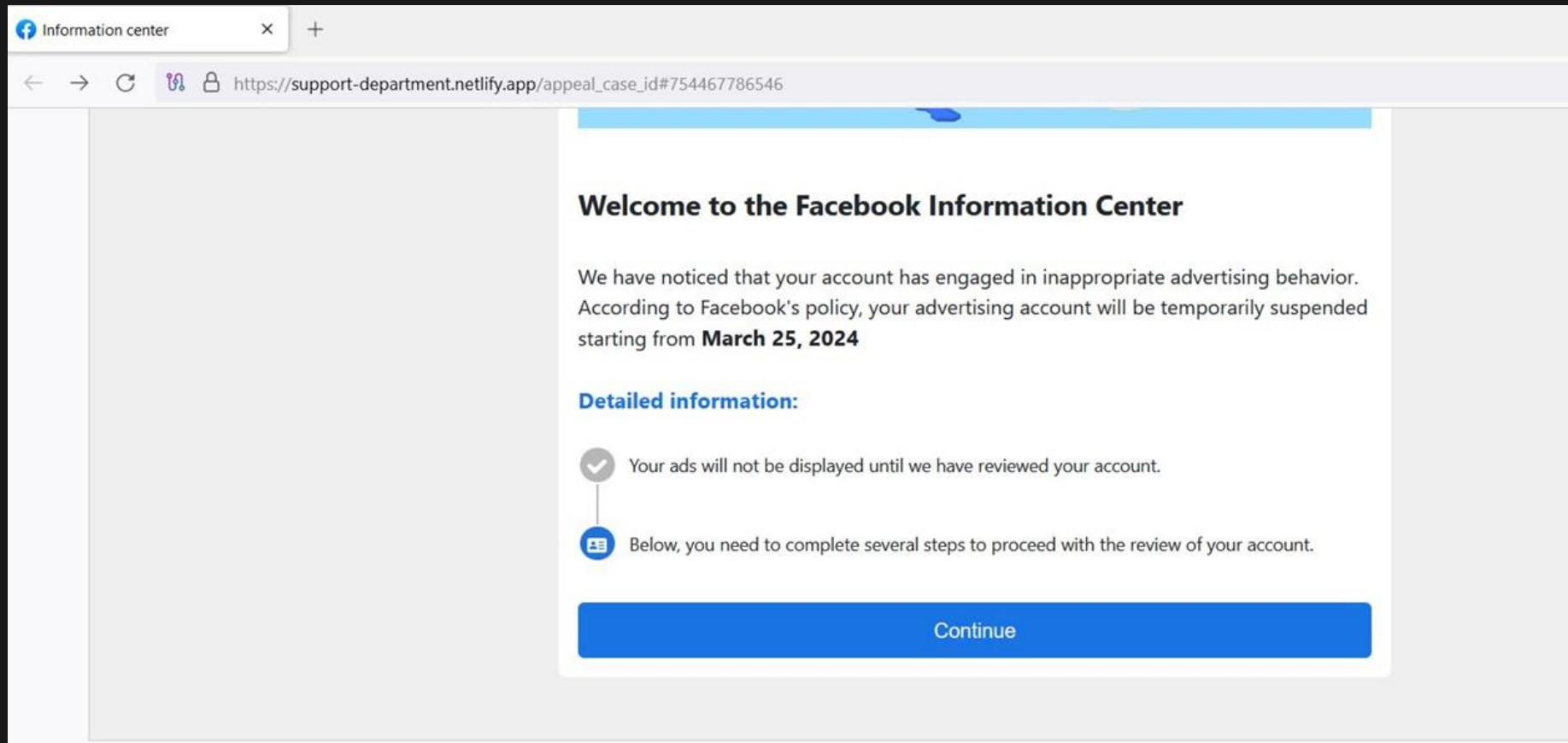
- Ύποπτο domain αποστολέα: Μπορεί ο αποστολέας να ισχυρίζεται πως είναι π.χ. το Facebook, αλλά αν εξετάσουμε το email από το οποίο στέλνει, ίσως καταλάβουμε ότι μάλλον κάτι δεν πάει και πολύ καλά.



- Αίσθηση του κατ' επείγοντος ή αίσθηση ενοχής: Οι επιτιθέμενοι προσπαθούν να δημιουργήσουν στο θύμα την ανάγκη να δράσει γρήγορα, γιατί αλλιώς θα υπάρξουν συνέπειες (κλείδωμα λογαριασμού) ή γιατί πραγματοποίησε παράνομες ενέργειες (εύρεση ύποπτου πορνογραφικού υλικού από την αστυνομία).

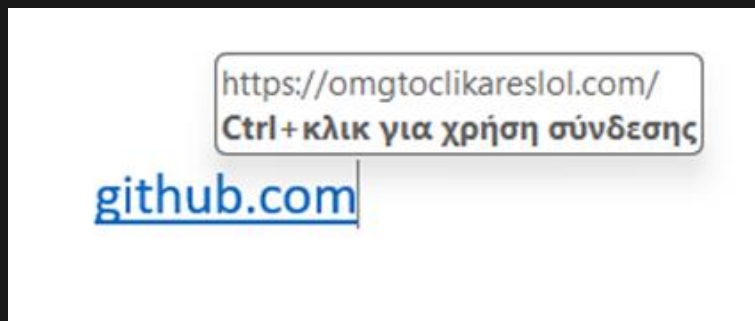


- Υποπτα links/attachments: Σύμφωνα, το wix και το netlify βοηθούν πολύ κόσμο να φτιάξει σελίδες, αλλά δε θα περιμέναμε να τα χρησιμοποιεί για παράδειγμα το Facebook



Προσέξτε ότι το συγκεκριμένο id μπορεί να χρησιμοποιείται ως tracing ώστε ο attacker να ενημερωθεί ότι το θύμα έκανε click to link

Προσοχή: Άλλο το κείμενο, άλλο το link



Επίσης, κατά 99% δε θα λάβεις χωρίς λόγο email από την Amazon με κάποιο .docx έγγραφο. Τα συνημμένα docs συνήθως χρησιμοποιούνται για εκτέλεση κακόβουλου κώδικα και είναι πιο πειστικά από ένα .exe αρχείο.

- Απάντηση σε μη ερώτηση: Ορισμένα emails αποστέλλονται με θέμα Re: (reply), χωρίς να έχει προηγηθεί κάποια συνομιλία με τον αποστολέα. Επίσης μπορεί να ενημερωθείτε ότι έχετε κερδίσει κάποιο βραβείο ή δώρο σε διαγωνισμό που δε συμμετείχατε ή που δεν υπάρχει.

FILE

MESSAGE

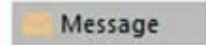


Fri 6/21/2019 7:54 AM

Google Official Winning Letter <winningalart@google.org>

Powered By Google ©

To Recipients



Message

📎 Official Winning Letter by Google andmastercard visa 2019.pdf

Dear Google User,

You have been selected as a winner for using Google services. Find attached email with more details.

Congratulations,

Eileen Naughton
Managing director of
UK & Ireland and vice president
Of people operations worldwide
On Behalf of

Larry Page
CEO & Co-Founder

©2019 Google - Terms & Privacy



- Επαλήθευση στοιχείων: Ένας πολύ μεγάλος αριθμός phishing scams όπως γνωρίζετε προσπαθούν να σας πείσουν να επιβεβαιώσετε τα στοιχεία σας π.χ. κωδικοί σε τράπεζες ή στο facebook, MFA, πιστωτικές κάρτες κτλ.

Εδώ πρέπει να θυμάστε ότι καμία τράπεζα και καμία Meta δε θα σας ζητήσει σε άκυρη χρονική στιγμή να επαληθεύσετε τους κωδικούς σας ή τα στοιχεία σας. Τέτοια emails είναι ξεκάθαρα scams και αν υπάρχει μία πιθανότητα να είναι ρεαλιστικά, τότε είναι προτιμότερο να επικοινωνήσετε με το support των sites για να εξακριβώσετε την αυθεντικότητά τους.

Τι μπορώ να κάνω ως αναλυτής;

Σίγουρα υπάρχουν πιο εξελιγμένοι τρόποι εξακρίβωσης ενός phishing scheme.

- Email Headers: Πρόκειται για τις επικεφαλίδες του email. Από αυτές λαμβάνουμε σημαντική πληροφορία, όπως για το από πού στέλνει ο attacker, αν είναι όντως αυτός που λέει ότι είναι κτλ.

Για παράδειγμα, τα ΕΛΤΑ θα ήταν περίεργο να στέλνουν από έναν random SMTP server της Αυστραλίας.

Η Microsoft παρέχει μια πολύ καλή σελίδα για ανάλυση headers, το Message Header Analyzer

← → ↻ 🔒 mha.azurewebsites.net

Message Header Analyzer

— Insert the message header you would like to analyze

X-ESHash: 80810362954852045903
X-AHash: 0
X-TID: 26475
X-EID: 3
X-RPCampaign: DollarGeneral22476023
X-TemplateID: 568
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="b1_81a6e0d83774c7653204fb72c08ccd60"
Content-Length: 52326

This is a multi-part message in MIME format.
--b1_81a6e0d83774c7653204fb72c08ccd60
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Analyze headers Clear Copy

#	Header	Value
1	Return-Path	<postmaster@etekno.xyz>
2	X-Originating-Ip	[209.85.167.226]
3	Received-SPF	none (domain of etekno.xyz does not designate permitted sender hosts)
4	Authentication-Asp	atlas105.free.mail.bf1.yahoo.com; dkim=unknown; spf=none smtp.mailfrom=etekno.xyz; dmarc=unknown header.from=JOq7ODDOwWdR-yVvCaBkTnp.qoqolecloud.com;

Authentication-Results		spf=fail (sender IP is 212.25.80.226)
Authentication-Results	spf=fail (sender IP is 212.25.80.226) smtp.mailfrom=o365info.com; o365info.com; dkim=none (message not signed) header.d=none;o365info.com; dmarc=fail action=none header.from=o365info.com;	
Received-SPF	Fail (protection.outlook.com: domain of o365info.com does not designate 212.25.80.226 as permitted sender) receiver=protection.outlook.com; client-ip=212.25.80.226; helo=DC01;	
3	Date	
4	From	

Fail (**protection.outlook.com**: domain of **o365info.com** does not designate **212.25.80.226** as permitted sender)

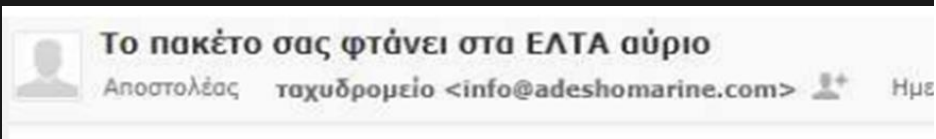
O365INFO.COM COPYRIGHT ©

- Η εγγραφή για το **SPF** (Sender Policy Framework) είναι επίσης πολύ σημαντική, καθώς μπορεί να φαίνεται ότι λαμβάνουμε ένα email από το o365info, αλλά το SPF authentication fail για το συγκεκριμένο domain μας λέει ότι η IP του αποστολέα δεν έχει άδεια να στείλει από αυτό το domain. Οπότε κάτι ύποπτο συμβαίνει.
- Αν ένας server δεν υποστηρίζει SPF authentication, τότε στην αντίστοιχη καταχώριση θα δούμε “None”.
- Εκτός από SPF, υπάρχουν οι μέθοδοι πιστοποίησης DKIM και DMARC που αξίζει να κοιτάξουμε.
- Περισσότερα εδώ

<https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/>

- Ανάλυση του domain / IP του αποστολέα: Μπορεί να γίνει μέσω εργαλείων όπως το whois.domaintools.com

Το παράδειγμα με τα ΕΛΤΑ



Whois Record for AdesHomarine.com	
— Domain Profile	
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com,http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) +1.4806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	1,886 days old Created on 2019-02-14 Expires on 2026-02-14 Updated on 2024-01-30
Name Servers	NS1.BLUEHOST.IN (has 88,918 domains) NS2.BLUEHOST.IN (has 88,918 domains)
Domain Status	Registered And No Website
IP History	8 changes on 8 unique IP addresses over 5 years
Registrar History	1 registrar with 1 drop
Hosting History	4 changes on 3 unique name servers over 5 years

Whois Record (last updated on 2024-04-14)

Όπως και με το Netlify, έτσι δε θα περιμέναμε από τα ΕΛΤΑ να χρησιμοποιούν email ή ιστοσελίδα μέσω GoDaddy.

- Επισκόπηση και σκανάρισμα της phishing ιστοσελίδας: Και αυτό μπορεί να γίνει με εργαλεία όπως το urlscan (καλό είναι να κάνουμε private scan και να προσέχουμε ώστε στο URL να έχουν αφαιρεθεί όλα τα στοιχεία tracing που πρόσθεσε attacker).

The screenshot displays the urlscan.io interface for a scan of **ieee.ntua.gr**. The URL is <https://ieee.ntua.gr/>. The scan was performed on April 14, 2024, at 11:13:51 am UTC, from Greece (GR) to Germany (DE). The summary indicates that the website contacted 4 IPs in 2 countries across 3 domains to perform 24 HTTP transactions. The main IP is 147.102.3.69, located in Athens, Greece, and belongs to NTUA, GR. The main domain is ieee.ntua.gr. The TLS certificate was issued by R3 on February 15th, 2024, and is valid for 3 months. The urlscan.io Verdict is 'No classification'. A live screenshot of the website is shown, featuring the IEEE NTUA logo and the text 'IT'S NOT FAITH IN TECHNOLOGY' and 'IT'S FAITH IN PEOPLE'. The page title is 'IEEE NTUA Student Branch'.

Summary

This website contacted 4 IPs in 2 countries across 3 domains to perform 24 HTTP transactions. The main IP is 147.102.3.69, located in Athens, Greece and belongs to NTUA, GR. The main domain is ieee.ntua.gr. TLS certificate: Issued by R3 on February 15th 2024. Valid for: 3 months.

This is the only time ieee.ntua.gr was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for ieee.ntua.gr

Current DNS A record: 147.102.3.69 (AS3323 - NTUA, GR)

Domain & IP information

Screenshot

Page Title

IEEE NTUA Student Branch

Εδώ μπορούμε να δούμε και ένα screenshot της σελίδας που τράβηξε το εργαλείο, χωρίς να χρειαστεί να την επισκεφτούμε εμείς οι ίδιοι.

- Σε βάθος ανάλυση των URLs και attachments:

- Προϋποθέτει να λάβουμε όλα τα απαιτούμενα μέτρα ασφαλείας για να μη μολυνθούμε σε περίπτωση κακόβουλου περιεχομένου. Για αυτό πρέπει να χρησιμοποιήσουμε ένα **sandbox environment**.
- Επίσης, πρέπει να διατηρήσουμε την IP και την τοποθεσία μας μυστική, οπότε καλό είναι να χρησιμοποιήσουμε VPN και Tor Browser.

Έχοντας λάβει τα απαραίτητα μέτρα, μπορούμε να εξετάσουμε πιο προσεκτικά την ιστοσελίδα, να δούμε τα connections της (web developer tools), για το πώς και πού αποστέλλονται τα δεδομένα, να δούμε αν γίνονται disclosed ευαίσθητες πληροφορίες (π.χ. Enabled Indexing) για τον attacker και να μάθουμε το infrastructure που χρησιμοποιεί.

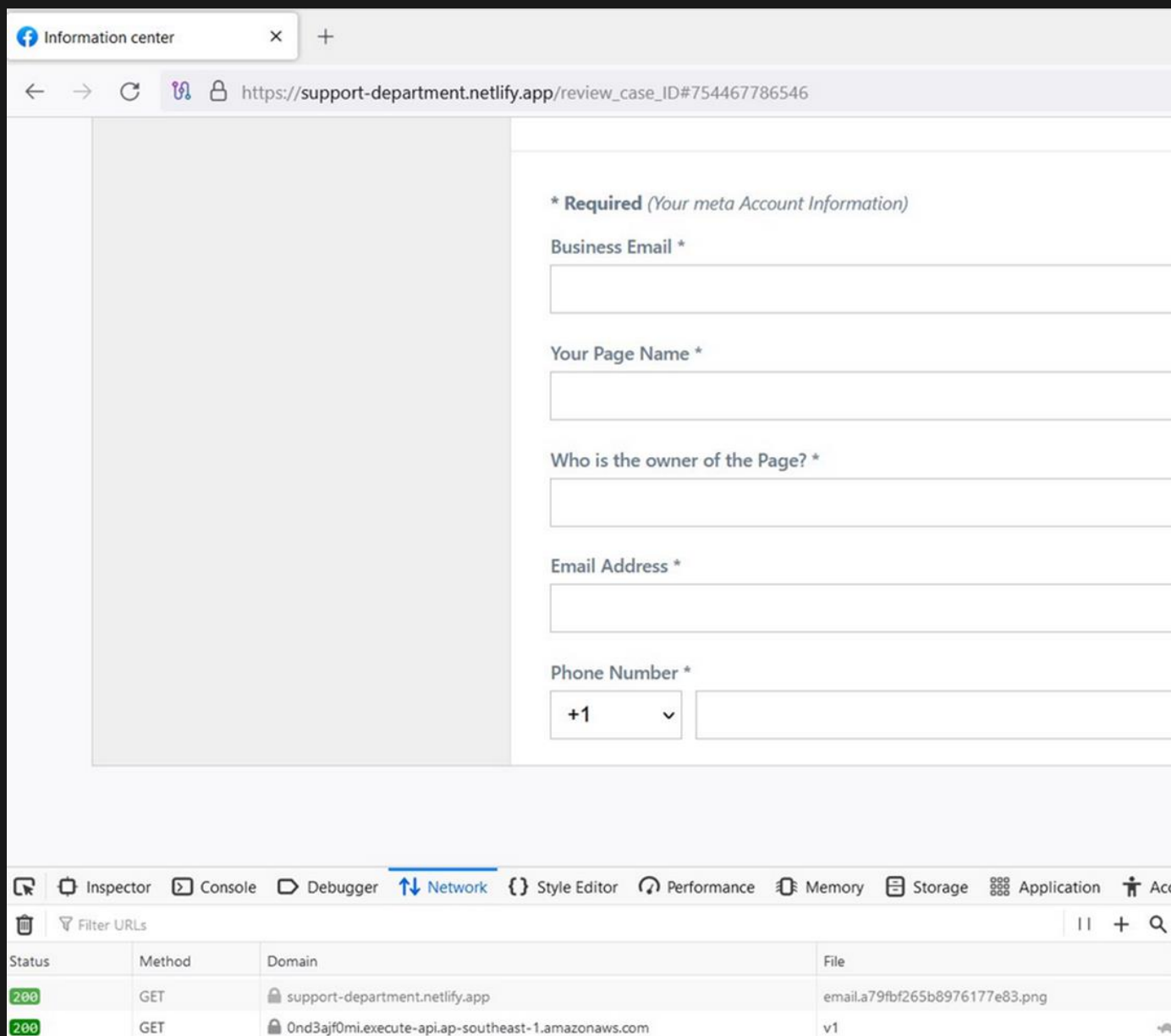
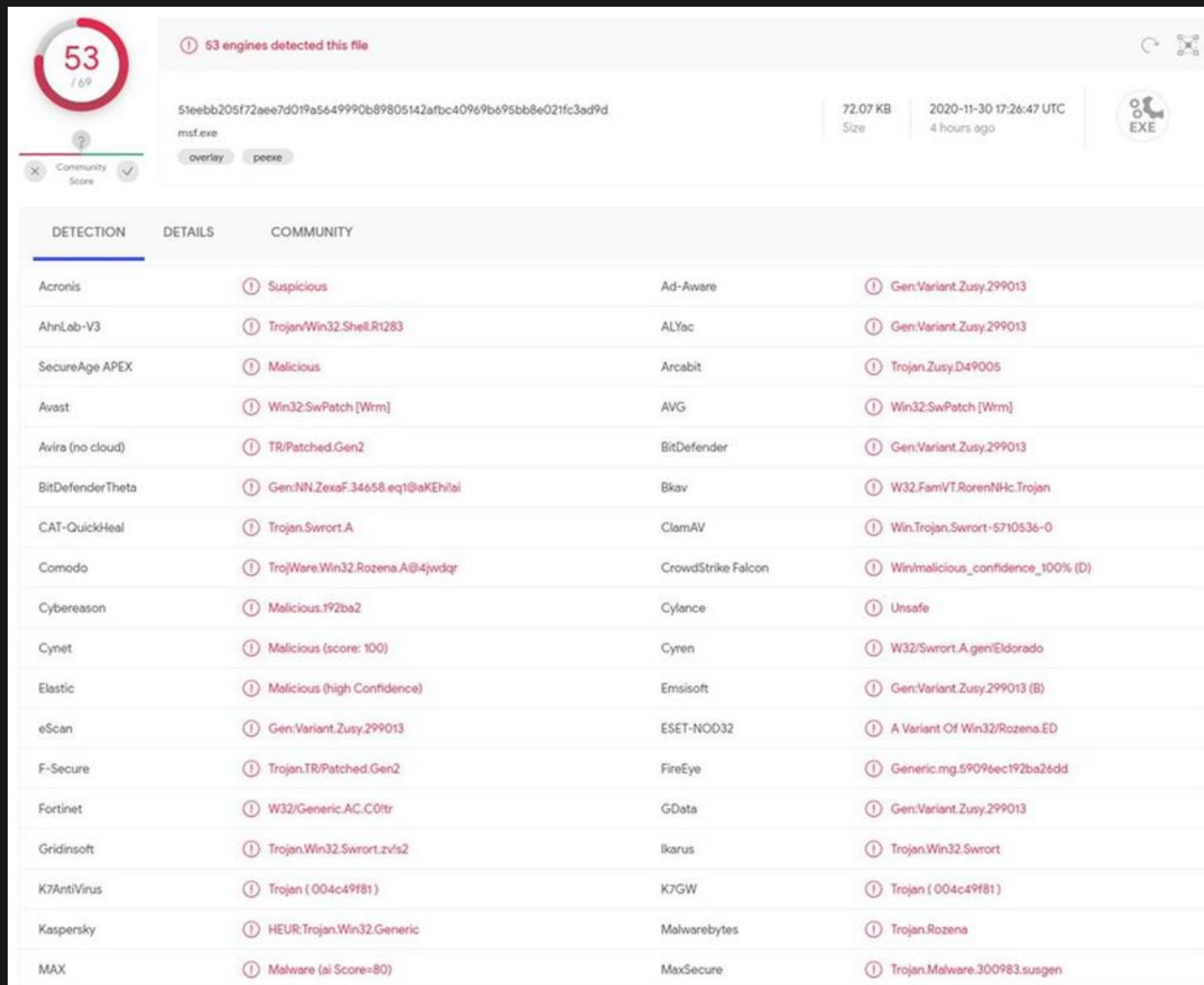


Photo by:

<https://twitter.com/v4ensics>

Το θύμα πραγματοποιεί
GET request στο api του
attacker στο aws

- Αν θέλουμε να αναλύσουμε attachments, τότε μπορούμε μέσω του **hash** τους να τα αναζητήσουμε σε ιστοσελίδες όπως το [VirusTotal](#). Πολλά malwares ανακυκλώνονται και έχουν ήδη σκαναριστεί, οπότε μια απλή αναζήτηση με βάση το hash είναι συνήθως αρκετή για να διαπιστώσουμε ότι ένα αρχείο είναι κακόβουλο.





53 engines detected this file

51eebb205f72aee7d019a5649990b89805142afbc40969b695bb8e021fc3ad9d
msf.exe
72.07 KB
2020-11-30 17:26:47 UTC
Size
4 hours ago
EXE



Community Score

DETECTION	DETAILS	COMMUNITY
Acronis	Suspicious	Ad-Aware Gen:Variant.Zusy.299013
AhnLab-V3	Trojan.Win32.Shell.R1283	ALYac Gen:Variant.Zusy.299013
SecureAge APEX	Malicious	Arcabit Trojan.Zusy.D49005
Avast	Win32:SwPatch [Wrm]	AVG Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2	BitDefender Gen:Variant.Zusy.299013
BitDefenderTheta	Gen:NN.ZexaF.34658.eq1@akEh!ai	Bkav W32.Fam!VT.RorenNHc.Trojan
CAT-QuickHeal	Trojan.Swrort.A	ClamAV Win.Trojan.Swrort-5710536-0
Comodo	TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon Win\malicious_confidence_100% (D)
Cybereason	Malicious.192ba2	Cylance Unsafe
Cynet	Malicious (score: 100)	Cyren W32/Swrort.A.gen!Eldorado
Elastic	Malicious (high Confidence)	Emsisoft Gen:Variant.Zusy.299013 (B)
eScan	Gen:Variant.Zusy.299013	ESET-NOD32 A Variant Of Win32/Rozena.ED
F-Secure	Trojan.TR/Patched.Gen2	FireEye Generic.mg.59096ec192ba26dd
Fortinet	W32/Generic.AC.C0!tr	GData Gen:Variant.Zusy.299013
Gridinsoft	Trojan.Win32.Swrort.zv!s2	Ikarus Trojan.Win32.Swrort
K7AntiVirus	Trojan (004c49f81)	K7GW Trojan (004c49f81)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes Trojan.Rozena
MAX	Malware (ai Score=80)	MaxSecure Trojan.Malware.300983.susgen



- Τέλος, σε περίπτωση που η αναζήτηση με βάση το hash δεν είναι αποτελεσματική (για παράδειγμα το αρχείο δεν αναγνωρίζεται στο VirusTotal) ή τα αποτελέσματα δε μας ικανοποιούν, μπορούμε να πραγματοποιήσουμε manual analysis, η οποία βέβαια προϋποθέτει τα κατάλληλα reverse engineering και forensics skills.

- Πέρα από αναζήτηση με βάση το hash, υπάρχει και η δυνατότητα scanning του αρχείου από το VirusTotal, αλλά πρέπει να έχετε υπόψιν ότι αν εμπλέκονται εμπιστευτικά δεδομένα, τότε το upload των αρχείων ίσως υπονομεύσει την εμπιστευτικότητα.



Οι πέντε πιο δαπανηρές επιθέσεις phishing μέχρι σήμερα

1. Facebook and Google

Μεταξύ 2013 και 2015, το Facebook και η Google εξαπατήθηκαν με ζημιά 100 εκατομμύρια δολάρια λόγω μιας εκτεταμένης καμπάνιας phishing. Ο phisher εκμεταλλεύτηκε το γεγονός ότι και οι δύο εταιρείες χρησιμοποίησαν την Quanta, μια εταιρεία με έδρα την Ταϊβάν, ως πωλητή. Ο εισβολέας έστειλε μια σειρά από πλαστά τιμολόγια στην εταιρεία που υποδύθηκε την Quanta, τα οποία πλήρωσαν τόσο το Facebook όσο και η Google.

2. Crelan Bank

Η Crelan Bank, στο Βέλγιο, έπεσε θύμα μιας απάτης με παραβίαση επιχειρηματικού email (BEC) που κόστισε στην εταιρεία περίπου 75,8 εκατομμύρια δολάρια. Αυτός ο τύπος επίθεσης περιλαμβάνει τον phisher που «παραβιάζει» τον λογαριασμό ενός στελέχους υψηλού επιπέδου μέσα σε μια εταιρεία και δίνει οδηγίες στους υπαλλήλους του να μεταφέρουν χρήματα σε έναν λογαριασμό που ελέγχεται από τον εισβολέα. Η επίθεση phishing της Crelan Bank ανακαλύφθηκε κατά τη διάρκεια εσωτερικού ελέγχου και ο οργανισμός μπόρεσε να απορροφήσει τη ζημία, καθώς διέθετε επαρκή εσωτερικά αποθέματα.

Οι πέντε πιο δαπανηρές επιθέσεις phishing μέχρι σήμερα

3. FACC

Η FACC, ένας Αυστριακός κατασκευαστής εξαρτημάτων αεροδιαστημικής, έχασε επίσης ένα σημαντικό χρηματικό ποσό από μια απάτη της BEC. Το 2016, η οργάνωση ανακοίνωσε την επίθεση και αποκάλυψε ότι ένας phisher που υποδύοταν τον διευθύνοντα σύμβουλο της εταιρείας έδωσε εντολή σε έναν υπάλληλο στο λογιστήριο να στείλει 61 εκατομμύρια δολάρια σε έναν τραπεζικό λογαριασμό που ελέγχεται από τους εισβολείς.

4. Upsher-Smith Laboratories

Το 2014, μια επίθεση της BEC εναντίον μιας φαρμακευτικής εταιρείας στη Μινεσότα είχε ως αποτέλεσμα την απώλεια άνω των 39 εκατομμυρίων δολαρίων. Ο phisher υποδύθηκε τον Διευθύνοντα Σύμβουλο των εργαστηρίων Upsher-Smith Laboratories και έστειλε email στον συντονιστή πληρωτέων λογαριασμών του οργανισμού με οδηγίες για την αποστολή ορισμένων τραπεζικών εμβασμάτων και για να ακολουθήσει τις οδηγίες ενός «δικηγόρου» που συνεργάζεται με τους εισβολείς.

Οι πέντε πιο δαπανηρές επιθέσεις phishing μέχρι σήμερα

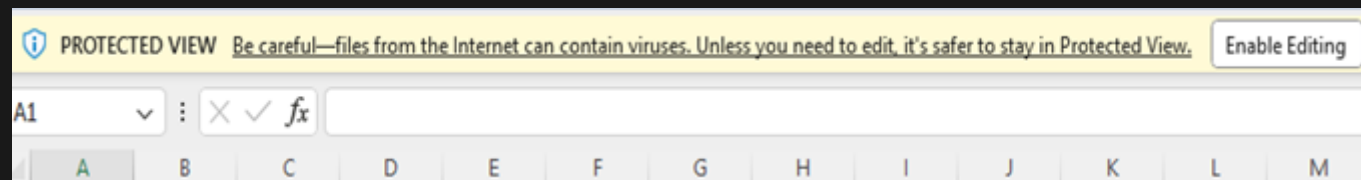
5. Ubiquiti Networks

Το 2015, η Ubiquiti Networks, μια εταιρεία δικτύων υπολογιστών με έδρα τις ΗΠΑ, έπεσε θύμα επίθεσης BEC που κόστισε στην εταιρεία 46,7 εκατομμύρια δολάρια (από τα οποία περίμεναν να ανακτήσει τουλάχιστον 15 εκατομμύρια δολάρια). Ο εισβολέας υποδύθηκε τον Διευθύνοντα Σύμβουλο και δικηγόρο της εταιρείας και έδωσε εντολή στον Γενικό Λογιστήριο της εταιρείας να κάνει μια σειρά από μεταφορές για να κλείσει μια μυστική εξαγορά. Κατά τη διάρκεια 17 ημερών, η εταιρεία πραγματοποίησε 14 τραπεζικά εμβάσματα σε λογαριασμούς στη Ρωσία, την Ουγγαρία, την Κίνα και την Πολωνία.

Exploitation Phase



Για το συγκεκριμένο παράδειγμα υποθέτουμε ότι χρήστης (**victim**) έχει ανοίξει το email και κατεβάσει το συνημμένο που περιέχεται. Με το άνοιγμα του αρχείου (για παράδειγμα Excel) εμφανίζεται ένα μήνυμα-προειδοποίηση για ενεργοποίηση των Macros αλλά επειδή δε γνωρίζει (αγνοεί) τι είναι επιλέγει να πατήσει “Ενεργοποίηση”.



Εφόσον ο χρήστης έχει ανοίξει το αρχείο και ο κώδικας εκτελεστεί, οι εξής συνηθισμένες περιπτώσεις υπάρχουν:

- Ο κώδικας να κατεβάσει από τον server του Threat Group ένα πιο εξελιγμένο malware το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί είτε για exfiltration και ransomware είτε για τη δημιουργία backdoors ώστε να μπορούν οι attackers να συνδεθούν οποιαδήποτε στιγμή.
- Ο κώδικας να προσπαθήσει να επικοινωνήσει απευθείας με τον server του attacker ώστε να αποκτήσει απευθείας πρόσβαση στο σύστημα.

Τα **Macros** και πιο συγκεκριμένα VBA macros είναι Visual Basic Application κώδικας ο οποίος εκτελεί ορισμένες εντολές μέσα σε συναρτήσεις που έχουν δημιουργηθεί σκόπιμα απο τον κακόβουλο χρήστη.

Σχεδόν πάντα ο κώδικας έχει υλοποιηθεί με τέτοιο τρόπο ώστε να ενεργοποιηθεί με το που ο χρήστης ανοίξει απλώς το αρχείο, χωρίς να κάνει τίποτα παραπάνω.

```
Private Sub Workbook_Open()
```

```
End Sub
```


Time for Live Demonstration

