ΕΝΑΣ ΟΔΗΓΟΣ ΤΗΣ ΚΟΙΝΟΤΗΤΑΣ PANOPTICPROTOCOL

The Lazarus Heist

Οι φάκελοι του Geoff White για τον κυβερνοστρατό της Βόρειας Κορέας, σε απλά ελληνικά — μαζί με τη Δεύτερη Ματιά

10 ΦΑΚΕΛΟΙ | ΑΠΛΑ ΕΛΛΗΝΙΚΑ | ΕΝΗΜΕΡΩΜΕΝΟ 2026

Μια χώρα που έμεινε χωρίς χρήματα έφτιαξε έναν στρατό για να τα κλέβει. Αυτό το βιβλίο είναι η ιστορία του πώς ένα πεινασμένο, αποκλεισμένο κράτος έμαθε μόνο του να ληστεύει τράπεζες με ένα πληκτρολόγιο — και των απλών ανθρώπων που το πλήρωσαν.

Ξαναχτίσαμε το βιβλίο σαν φακέλους υποθέσεων: το κίνητρο, επτά επιχειρήσεις, η κλιμάκωση, η ετυμηγορία. Κάθε φάκελος κλείνει με τη **Δεύτερη Ματιά** — τι έγινε αφού ο White έκλεισε το χειρόγραφο το 2021 — και το μάθημα που αφήνει σε όποιον κρατά κρύπτο σήμερα.

Συνοδευτικός οδηγός, όχι αντικατάσταση — αν σε κερδίσει μια υπόθεση, αγόρασε το βιβλίο.

ΣΥΝΕΡΓΑΣΟΥ ΜΕ ΤΟ PANOPTICPROTOCOL

Συμβουλευτική για Ιδιώτες — προσωπική καθοδήγηση ένας προς έναν στα κρύπτο, χτισμένη πάνω στους στόχους και στο ρίσκο σου.

Συμβουλευτική για Επιχειρήσεις — στρατηγική, υιοθέτηση και συμβουλές κρύπτο για εταιρείες και ομάδες.

Περιεχόμενα

> *Πλήρης έκδοση — όλο το βιβλίο σε απλά ελληνικά, συν πέντε χρόνια που το βιβλίο δεν πρόλαβε. Συνοδευτικός οδηγός, όχι αντικατάσταση: αγόρασε το βιβλίο. Μόνο εκπαιδευτικό. NFA. DYOR.*

ΦΑΚΕΛΟΣ 00

Η Χώρα που Έμεινε από Χρήματα

Γιατί ένα πυρηνικό κράτος άρχισε να ληστεύει τράπεζες. Καλύπτει την Εισαγωγή και τα κεφάλαια 2–3.

ΥΠΟΘΕΣΗ: Η ΟΙΚΟΝΟΜΙΑ ΤΗΣ Β. ΚΟΡΕΑΣ · **ΕΤΗ:** 1948–2006 · **ΚΑΤΑΣΤΑΣΗ:** ΕΓΚΛΗΜΑ ΩΣ ΚΡΑΤΙΚΗ ΠΟΛΙΤΙΚΗ

Οι περισσότερες κυβερνοδυνάμεις χακάρουν για μυστικά. Η Βόρεια Κορέα χακάρει για μετρητά — και το πρώτο επιχείρημα του White είναι ότι δεν καταλαβαίνεις το χακάρισμα αν δεν καταλάβεις τη χρεοκοπία από πίσω. Ένα κράτος που ιδρύθηκε το 1948 κλειδώθηκε σε αυτό που ονομάζει **φαινόμενα καστάνιας**: έναν πόλεμο που δεν μπορούσε ούτε να κερδίσει ούτε να παραδεχτεί, μια ιδεολογία αυτάρκειας που απαγόρευε τη βοήθεια, και μια απομόνωση τόσο πλήρη ώστε κάθε χρόνο ο κόσμος έξω απομακρυνόταν κι άλλο.

Ο λογαριασμός ήρθε τη δεκαετία του 1990. Οι σοβιετικές επιδοτήσεις σταμάτησαν και το σύστημα τροφίμων κατέρρευσε. Οι εκτιμήσεις για τους νεκρούς πάνε από 240.000 έως τρία εκατομμύρια. Η Jihyun Park, που δραπέτευσε και ζει σήμερα στην Αγγλία, θυμάται να πιάνει λιβελούλες με τους συμμαθητές της και να τις τρώει. Θυμάται και το πρώτο πτώμα: έναν δεκατριάχρονο μαθητή της που ήθελε να γίνει γιατρός. Κανείς δεν έλεγε «λιμός». Έλεγαν ότι ο νεκρός *είχε μια αρρώστια*.

Ο Αμερικανός αναλυτής David Asher πέρασε χρόνια πάνω σε μία ερώτηση: με δεκαετές εμπορικό έλλειμμα και σχεδόν ολική χρεοκοπία, *από πού έβρισκαν τα λεφτά;* Η απάντηση ήταν το έγκλημα, οργανωμένο σαν κρατικό υπουργείο. Πλαστό Viagra, πλαστά τσιγάρα, μεθαμφεταμίνη, και πάνω απ' όλα το **«superdollar»**: ένα πλαστό χαρτονόμισμα των 100 δολαρίων τόσο καλό ώστε, όταν μυστικός πράκτορας του FBI έστειλε δείγμα για ανάλυση, το εργαστήριο απάντησε ότι είναι γνήσιο. Δεκαπέντε χρόνια έρευνας, μια επιχείρηση-παγίδα στημένη σαν γάμος σε θαλαμηγό, πενήντα εννέα συλλήψεις από Κίνα, Ταϊβάν, Καναδά και ΗΠΑ — και ούτε ένας Βορειοκορεάτης. Η συνήθης εξήγηση: όσοι Βορειοκορεάτες ταξιδεύουν είναι κρατικοί υπάλληλοι με διπλωματική ασυλία.

Η Δεύτερη Ματιά: γύρω στο 2006 τα superdollars ξεθώριασαν. Όχι επειδή άλλαξε η πολιτική, αλλά επειδή άλλαξε το μέσο. Το χρήμα πήγαινε online, και ένα κράτος ήδη οργανωμένο γύρω από παράνομα έσοδα απλώς το ακολούθησε. Όλα όσα ακολουθούν είναι η ίδια επιχείρηση, ξαναχτισμένη για το ίντερνετ.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Δεν είναι συμμορία, είναι κονδύλι προϋπολογισμού.** Δεν αποτρέπεται κάνοντας την κλοπή ασύμφορη, γιατί η εναλλακτική δεν είναι άλλη δουλειά — είναι εθνική πτώχευση.
2. **Η αποποίηση ευθύνης ήταν σχεδιασμένη από την αρχή.** Διπλωματικά διαβατήρια τότε, εταιρείες-βιτρίνες και δανεικές ταυτότητες τώρα.

> **Η ΟΥΣΙΑ**
>
> *Ένα κράτος που δεν μπορεί να βγάλει λεφτά νόμιμα, θα φτιάξει κάτι που τα παίρνει. Αυτό το κάτι δείχνει τώρα στα κρύπτο.*

ΦΑΚΕΛΟΣ 01

Dark Seoul: Πρόβα στον Γείτονα

Εκεί που η ομάδα έμαθε να καταστρέφει — και να φοράει μάσκες. Καλύπτει το κεφάλαιο 4.

ΣΤΟΧΟΣ: ΤΡΑΠΕΖΕΣ & ΚΑΝΑΛΙΑ Ν. ΚΟΡΕΑΣ · **ΕΤΟΣ:** 2013 · **ΖΗΜΙΑ:** 32.000 ΥΠΟΛΟΓΙΣΤΕΣ

Στις 2 το μεσημέρι της Τετάρτης 20 Μαρτίου 2013, τριάντα δύο χιλιάδες υπολογιστές σε δύο από τις μεγαλύτερες τράπεζες της Νότιας Κορέας και στα τρία μεγαλύτερα κανάλια της έσβησαν την ίδια στιγμή. Το κακόβουλο λογισμικό χτύπησε το **Master Boot Record** — την εντολή που λέει στο μηχάνημα πού να βρει το ίδιο του το λειτουργικό. Χωρίς MBR, δεν υπάρχει υπολογιστής. ATM και e-banking έπεσαν· τα συστήματα ξαναχτίστηκαν ένα-ένα.

Δύο πράγματα ανησύχησαν τους αναλυτές. Πρώτον, η κλιμάκωση: η στρατιωτική θεωρία μιλά για πέντε επιλογές απέναντι σε έναν εχθρό — άρνηση, υποβάθμιση, διατάραξη, παραπλάνηση, καταστροφή — και οι επιτιθέμενοι πήγαν κατευθείαν στην τελευταία. Δεύτερον, οι μάσκες. Η αρχική σελίδα μιας εταιρείας κινητής τηλεφωνίας παραμορφώθηκε με κόκκινα κρανία υπογεγραμμένα **«Whois Team»**. Την επόμενη μέρα μια ομάδα με το όνομα **NewRomantic Cyber Army Team** ανέλαβε την ευθύνη για τις τράπεζες. Κανένα από τα δύο ονόματα δεν είχε υπάρξει ποτέ πριν, ούτε εμφανίστηκε ποτέ ξανά. Οι ερευνητές βρήκαν αργότερα ότι ο κώδικας τα συνέδεε — και τα δύο με την ίδια επιχείρηση.

Η απόδοση ευθύνης βασίστηκε σε βορειοκορεατικές διευθύνσεις IP μέσα στον κώδικα — αδύναμη ένδειξη στις περισσότερες χώρες, ασυνήθιστα ισχυρή εδώ, γιατί κανένα εμπορικό VPN δεν σου προσφέρει έξοδο από τη Βόρεια Κορέα. Και τα εργαλεία οδηγούσαν πίσω στο 2009, σε λογισμικό που κατασκόπευε αθόρυβα τις ένοπλες δυνάμεις της Νότιας Κορέας. Οι επιτιθέμενοι μπορούσαν να σβήσουν και εκείνα τα μηχανήματα. Επέλεξαν να μην το κάνουν.

Η Δεύτερη Ματιά: η αυτοσυγκράτηση είναι το εύρημα. Δεκατρία χρόνια μετά, ιοί της Βόρειας Κορέας κάθονται μέσα σε συστήματα που ποτέ δεν πυροδότησαν. Όπως το έθεσε ο πρώην πρέσβης Thae Yong Ho: σε καιρό ειρήνης οι χάκερ βγάζουν χρήματα· σε καιρό πολέμου η ίδια πρόσβαση γίνεται όπλο. Κάθε ληστεία σε αυτόν τον οδηγό είναι και μια πρόβα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Η ομάδα κρύβεται πίσω από επινοημένα ονόματα.** Μια επίθεση που «ανέλαβε» μια άγνωστη ακτιβιστική ομάδα δεν αποδεικνύει ποιος το έκανε. Συχνά δείχνει ποιος θέλει να κοιτάς αλλού.
2. **Το wiper δεν ζητά λύτρα και δεν επιστρέφει τίποτα.** Αντίγραφα ασφαλείας που ζουν στο ίδιο δίκτυο δεν είναι αντίγραφα ασφαλείας.

> **Η ΟΥΣΙΑ**
>
> *Έκαναν πρόβα στον γείτονα πρώτα — και ο κόσμος το πέρασε για τοπική είδηση.*

ΦΑΚΕΛΟΣ 02

Χακάροντας το Χόλιγουντ

Μια κωμωδία για τον Κιμ Γιονγκ Ουν, 38 εκατομμύρια κλεμμένα αρχεία, και η ταχύτερη απόδοση ευθύνης στην ιστορία των κυβερνοεπιθέσεων. Καλύπτει τα κεφάλαια 5–6.

ΣΤΟΧΟΣ: SONY PICTURES · **ΕΤΟΣ:** 2014 · **ΕΙΣΟΔΟΣ:** ENA PHISHING LINK

Στις 25 Σεπτεμβρίου 2014 κάποιος με το όνομα «Nathan Gonsalez» έστειλε σε υπάλληλο της Sony έναν σύνδεσμο με αρχεία βίντεο για μια διαφημιστική καμπάνια. Κάποιος τα κατέβασε. Οι επιτιθέμενοι πέρασαν μετά δύο μήνες μετακινούμενοι αθόρυβα από μηχάνημα σε μηχάνημα, πριν τα πυροδοτήσουν όλα μαζί στις 24 Νοεμβρίου. Οι κάρτες εισόδου έπαψαν να δουλεύουν. Οκτώ χιλιάδες μηχανήματα αποσυνδέθηκαν. Έξι εβδομάδες μετά, η καφετέρια του στούντιο ακόμα δεν δεχόταν κάρτα. Οι εργαζόμενοι έκαναν ουρά στο πάρκινγκ για χάρτινες επιταγές μισθοδοσίας.

Αυτό που ακολούθησε δεν ήταν τόσο χακάρισμα όσο καμπάνια επικοινωνίας. Οι επιτιθέμενοι, με το όνομα **Guardians of Peace**, είχαν πάρει περίπου **38 εκατομμύρια αρχεία** και τα έδωσαν σε δημοσιογράφους σε οκτώ χρονισμένα κύματα — πρώτα ακυκλοφόρητες ταινίες για να χτίσουν κοινό, μετά μισθοί, μετά 5.000 email της συν-προέδρου Amy Pascal. Διάλεξαν μεσαίου μεγέθους ιστοσελίδες που θα έβγαζαν τα θέματα, και τα μεγάλα δίκτυα θα τα κυνηγούσαν μετά. Στις 16 Δεκεμβρίου επικαλέστηκαν την 11η Σεπτεμβρίου εναντίον κάθε κινηματογράφου που θα έπαιζε την ταινία· οι αλυσίδες την απέσυραν, και στις 19 Δεκεμβρίου ο πρόεδρος Ομπάμα είπε δημόσια ότι το έκανε η Βόρεια Κορέα — ποτέ, σημειώνει ο White, δεν είχε ηγέτης μεγάλης δύναμης κατηγορήσει τόσο γρήγορα άλλη χώρα για συγκεκριμένη κυβερνοεπίθεση.

Το τίμημα δεν το πλήρωσαν τα στελέχη. Η υπάλληλος Celina Chavanette βρήκε online το συμβόλαιό της, τον μισθό της και τον αριθμό κοινωνικής ασφάλισής της: *«Το πληρώνω για πάντα.»* Η Amy Heller, που είχε απολυθεί επτά μήνες πριν, βρήκε μια εσωτερική αναφορά για ένα χαμένο εργονομικό ποντίκι αξίας 90 δολαρίων, καταχωρημένη ως «εγκλημα κατά περιουσίας» — αρκετό, σε έναν κλάδο όπου σε ψάχνουν στο Google, για να τελειώσει μια καριέρα.

Η Δεύτερη Ματιά: η ετυμηγορία της πρώην αναλύτριας της NSA Priscilla Moriuchi άντεξε καλύτερα. Ο κόσμος διάβασε την επίθεση ως παράλογη υπερβολή για μια χαζή ταινία και υποβάθμισε την απειλή. Έπρεπε να διαβάσει την τεχνική: μια ομάδα που ήξερε ότι το πραγματικό φορτίο ήταν *τα ενοχλητικά email των στελεχών*, όχι οι ταινίες.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Ένας άνθρωπος, ένα κλικ, ένα δίκτυο τελειωμένο.** Κάθε υπόθεση σε αυτό το βιβλίο ξεκινά έτσι. Δεύτερο μάθημα δεν υπάρχει.
2. **Τα κλεμμένα δεδομένα δεν λήγουν.** Οι εργαζόμενοι της Sony ζουν ακόμα με το 2014.

> **Η ΟΥΣΙΑ**
>
> *Δεν έσπασαν απλώς το δίκτυο. Κατάλαβαν το κοινό.*

ΦΑΚΕΛΟΣ 03

Η Ληστεία του Ενός Δισεκατομμυρίου

Ένας χρόνος μέσα σε κεντρική τράπεζα, ένας σαμποταρισμένος εκτυπωτής, και το ημερολόγιο που παραλίγο να τους το χαρίσει. Καλύπτει τα κεφάλαια 7–8.

ΣΤΟΧΟΣ: ΤΡΑΠΕΖΑ ΤΟΥ ΜΠΑΝΓΚΛΑΝΤΕΣ · **ΕΤΟΣ:** 2016 · **ΑΠΟΠΕΙΡΑ:** $951ΕΚ · **ΚΛΑΠΗΚΑΝ:** $101ΕΚ

Στις 29 Ιανουαρίου 2015 ένα ευγενικό email από τον «Rasel Ahlam» έφτασε σε υπαλλήλους της Τράπεζας του Μπανγκλαντές, ζητώντας τους να κατεβάσουν ένα βιογραφικό. Κάποιος το έκανε. Ακριβώς έναν χρόνο αργότερα — 29 Ιανουαρίου 2016 — οι επιτιθέμενοι έφτασαν στο τερματικό του **SWIFT**, του συστήματος με το οποίο οι τράπεζες μετακινούν χρήματα. Αντικατέστησαν δύο bytes του λογισμικού με εντολές που δεν κάνουν τίποτα, ώστε ένας έλεγχος που έπρεπε να λέει «όχι» να λέει πάντα «ναι» — και πείραξαν τον εκτυπωτή που έβγαζε τα χάρτινα αρχεία ώστε να τυπώνει λευκές σελίδες.

Μετά χρησιμοποίησαν το ημερολόγιο. Οι μεταφορές ξεκίνησαν στις 8.36 το βράδυ της Πέμπτης 4 Φεβρουαρίου, ώρα Ντάκα — τριάντα τρία λεπτά αφότου έφυγε ο υπεύθυνος βάρδιας, και 9.36 το πρωί στη Νέα Υόρκη. Το Σαββατοκύριακο στο Μπανγκλαντές είναι Παρασκευή–Σάββατο· στη Νέα Υόρκη Σάββατο–Κυριακή· και η Δευτέρα 8 Φεβρουαρίου ήταν η πρώτη μέρα της κινεζικής Πρωτοχρονιάς στη Μανίλα. Τρία ημερολόγια, το ένα πάνω στο άλλο, τους χάρισαν πέντε μέρες προβάδισμα. Τριάντα πέντε εντολές έφυγαν για **$951 εκατομμύρια** — σχεδόν όλο τον λογαριασμό.

Τους σταμάτησε η τύχη. Το υποκατάστημα στη Μανίλα που είχαν διαλέξει βρισκόταν στην **οδό Jupiter**, και «Jupiter» λέγεται και ένα κυρωμένο ιρανικό πλοίο. Η λέξη χτύπησε συναγερμό στα αυτόματα συστήματα της Fed, ένας υπάλληλος έλεγξε όλη τη δέσμη, και τριάντα μεταφορές μπλοκαρίστηκαν. Πέρασαν πέντε: **$101 εκατομμύρια**. Οι χάκερ δεν ήταν παντοδύναμοι, γράφει ο White — ήταν *«ένας διαρρήκτης πεταμένος στη μέση ενός σκοτεινού σπιτιού με έναν αδύναμο φακό»*.

Η Δεύτερη Ματιά: το FBI κατηγόρησε τον Park Jin Hyok το 2018 και πρόσθεσε τους Jon Chang Hyok και Kim Il το 2021, για απόπειρες άνω του $1,2 δισ. σε τράπεζες Ασίας, Αφρικής, Ευρώπης και Λατινικής Αμερικής. Κανείς δεν συνελήφθη ποτέ. Στο μεταξύ η τακτική μετανάστευσε: το τερματικό SWIFT του 2016 είναι το hot wallet του ανταλλακτηρίου σήμερα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Η υπομονή είναι το σημάδι.** Οι σοβαροί επιτιθέμενοι περιμένουν έναν χρόνο. Αν ο μόνος σου έλεγχος είναι «έγινε κάτι σήμερα;», θα τους χάσεις.
2. **Και τα δύο αντίγραφα έπεσαν μαζί.** Το ψηφιακό αρχείο και η χάρτινη εκτύπωση ήταν ο ίδιος έλεγχος δύο φορές.

> **Η ΟΥΣΙΑ**
>
> *Μια σύμπτωση έσωσε το 90% των χρημάτων. Όχι ένας μηχανισμός ασφαλείας. Μια σύμπτωση.*

ΦΑΚΕΛΟΣ 04

Η Διαφυγή: Καζίνο, Μετρητά κι ένα Ορθογραφικό

Η κλοπή ήταν το εύκολο κομμάτι. Καλύπτει τα κεφάλαια 9–12.

ΔΙΑΔΡΟΜΗ: ΜΑΝΙΛΑ & ΚΟΛΟΜΠΟ · **ΕΤΟΣ:** 2016 · **ΑΝΑΚΤΗΘΗΚΕ:** ΕΛΑΧΙΣΤΟ

Από τα $101 εκατ., τα **$81 εκατ.** προσγειώθηκαν σε τέσσερις λογαριασμούς σε υποκατάστημα της RCBC στην οδό Jupiter, ανοιγμένους εννέα μήνες νωρίτερα με πλαστά διπλώματα οδήγησης από κατόχους που δήλωναν όλοι την ίδια θέση εργασίας και τον ίδιο μισθό. Το κλειστό κύκλωμα του υποκαταστήματος είχε χαλάσει την προηγούμενη μέρα και επισκευάστηκε την επόμενη Τρίτη. Όταν η τράπεζα πάγωσε επιτέλους τους λογαριασμούς, από τα $81 εκατ. είχαν απομείνει **$68.335**.

Τα χρήματα έγιναν μετρητά — μισό δισεκατομμύριο πέσος, περίπου 500 κιλά, το βάρος ενός πιάνου με ουρά — και τα παρέλαβαν δύο Κινέζοι με ένα βαν. Τριάντα εκατομμύρια πήγαν σε έναν άνδρα ονόματι Weikang Xu, που έφυγε από τη χώρα και δεν ξαναεμφανίστηκε ποτέ. Τα υπόλοιπα πήγαν στα καζίνο **Solaire** και **Midas**, όπου ο νόμος των Φιλιππίνων τότε εξαιρούσε τα καζίνο από τους κανόνες κατά του ξεπλύματος. Δεκάδες παίκτες κάθισαν σε ιδιωτικές αίθουσες επί *εβδομάδες*, παίζοντας μπακαρά με ισορροπημένα στοιχήματα για να ανακτήσουν περίπου 90 σεντς στο δολάριο, ενώ η ιστορία έπαιζε στα πρωτοσέλιδα γύρω τους.

Η πέμπτη μεταφορά πήγε στη Σρι Λάνκα — **$20 εκατ.** σε ένα μικρό φιλανθρωπικό ίδρυμα, το Shalika Foundation, για μια φάρμα γαλακτοκομικών που δεν είχε ποτέ χτιστεί και που ο ίδιος ο ιστότοπός τους κοστολογούσε κάτω από $1 εκατ. Ένας υπάλληλος τράπεζας πρόσεξε ότι ο δικαιούχος έγραφε **«Shalika Fundation»**. Τα χρήματα γύρισαν πίσω. Η άβολη παρατήρηση του White: από όλους όσους πιάστηκαν σε αυτόν τον μηχανισμό, οι δύο που καταδικάστηκαν ή καταστράφηκαν ήταν γυναίκες — μια διευθύντρια υποκαταστήματος και μια διευθύντρια ιδρύματος — ενώ οι άνδρες που κουβάλησαν τα μετρητά εξαφανίστηκαν.

Η Δεύτερη Ματιά: εδώ φαίνεται γιατί τα κρύπτο μετρούν στην ιστορία. Το ξέπλυμα $51 εκατ. χρειάστηκε μια διεφθαρμένη διευθύντρια, ένα ανταλλακτήριο συναλλάγματος, δύο κούριερ, δεκάδες παίκτες και αρκετές εβδομάδες. Το 2017 η ίδια ομάδα ξέπλυνε τα λύτρα του WannaCry σε λιγότερο από 48 ώρες, χωρίς κανέναν άνθρωπο.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Η μετακίνηση κλεμμένων χρημάτων είναι πιο δύσκολη από την κλοπή.** Γι’ αυτό κάθε προσπάθεια ανάκτησης στοχεύει την έξοδο.
2. **Τον νομικό κίνδυνο τον σηκώνουν οι μεσάζοντες.** Ποτέ μη μετακινείς κεφάλαια για κάποιον του οποίου την πηγή δεν μπορείς να επαληθεύσεις.

> **Η ΟΥΣΙΑ**
>
> *Ένα ορθογραφικό έσωσε $20 εκατομμύρια. Τόσο λεπτά είναι τα περιθώρια αυτής της δουλειάς.*

ΦΑΚΕΛΟΣ 05

WannaCry

Ένα κλεμμένο όπλο της NSA, 230.000 μηχανήματα, 7.000 ακυρωμένα ραντεβού στο NHS — και λύτρα που μόλις έφταναν για ένα αυτοκίνητο. Καλύπτει το κεφάλαιο 13.

ΗΜΕΡΟΜΗΝΙΑ: 12 ΜΑΪΟΥ 2017 · **ΕΞΑΠΛΩΣΗ:** 150 ΧΩΡΕΣ · **ΖΗΜΙΑ:** $4–8 ΔΙΣ.

Ο Patrick Ward, σαράντα επτά ετών, περίμενε δύο χρόνια για εγχείρηση ανοιχτής καρδιάς. Λίγα λεπτά πριν ξεκινήσει, ο χειρουργός του είπε ότι οι υπολογιστές του νοσοκομείου είχαν χαθεί και η επέμβαση ακυρώθηκε. Σε όλη την Αγγλία, το ένα τρίτο των οργανισμών που διοικούν νοσοκομεία του NHS είτε μολύνθηκαν είτε αναγκάστηκαν να αποσυνδεθούν. Ακυρώθηκαν σχεδόν **7.000 ραντεβού**, πάνω από εκατό εκ των οποίων επείγοντα ογκολογικά.

Αυτό που έκανε το WannaCry διαφορετικό ήταν ότι εξαπλωνόταν μόνο του. Πάνω σε ένα συνηθισμένο ransomware ήταν βιδωμένα τα **EternalBlue** και **DoublePulsar** — εργαλεία φτιαγμένα από την αμερικανική NSA, που γνώριζε το κενό ασφαλείας των Windows από το 2012 και το κρατούσε, ώσπου μια ομάδα με το όνομα Shadow Brokers τα έκλεψε και τα δημοσίευσε τον Απρίλιο του 2017. Η Microsoft είχε βγάλει διόρθωση. Δεν ήταν υποχρεωτική. Εκατομμύρια μηχανήματα ήταν εκτεθειμένα.

Το σταμάτησε ένας 22χρονος στο Ντέβον. Ο Marcus Hutchins, ξεψαχνίζοντας τον κώδικα μετά το μεσημεριανό του, πρόσεξε ότι ο ιός έλεγχε αν υπήρχε ένα συγκεκριμένο αδήλωτο domain και σταματούσε αν υπήρχε. Το αγόρασε για κάτω από £10. Οι μολύνσεις σταμάτησαν μέσα σε δευτερόλεπτα. Ήταν ένα φρένο ασφαλείας του προγραμματιστή που κανείς δεν είχε αφαιρέσει — μία από τις ενδείξεις ότι το πράγμα κυκλοφόρησε ημιτελές. Άλλη μία: αντί για ένα πορτοφόλι ανά θύμα, ο κώδικας είχε μόλις **τρεις διευθύνσεις Bitcoin**.

Η Δεύτερη Ματιά: τα λύτρα ήταν λίγες εκατοντάδες χιλιάδες δολάρια — καταστροφή με τα μέτρα του ransomware. Το επιχείρημα του White είναι ότι το κέρδος δεν ήταν ποτέ ο σκοπός. Στις 3 Αυγούστου 2017 και τα τρία πορτοφόλια άδειασαν μέσα σε λίγα λεπτά, πέρασαν από δεκάδες διευθύνσεις και κατέληξαν σε ανταλλακτήριο, όπου τα ίχνη χάθηκαν. Το WannaCry μοιάζει με αποτυχία. Ήταν πρόβα ξεπλύματος.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Οι ενημερώσεις δεν είναι γραφειοκρατία.** Η διόρθωση υπήρχε μήνες. Όλα όσα ακολούθησαν ήταν προαιρετικά.
2. **Κρίνε μια επιχείρηση από το τι έμαθε ο επιτιθέμενος, όχι από το τι κέρδισε.** Ένα «αποτυχημένο» χακάρισμα που αποδεικνύει νέα διαδρομή ξεπλύματος είναι νίκη για εκείνους.

> **Η ΟΥΣΙΑ**
>
> *Ο κόσμος το είπε αποτυχημένη ληστεία. Ήταν μια πετυχημένη γενική πρόβα.*

ΦΑΚΕΛΟΣ 06

Παλιά Κόλπα, Νέο Χρήμα

Η ψεύτικη εφαρμογή trading, ο ψεύτικος recruiter, η ψεύτικη εταιρεία — το εγχειρίδιο των κρύπτο, γραμμένο το 2018. Καλύπτει το κεφάλαιο 14.

ΣΤΟΧΟΙ: ΑΝΤΑΛΛΑΚΤΗΡΙΑ & ΙΔΙΩΤΕΣ · **ΕΤΗ:** 2017–2020 · **ΣΥΝΟΛΟ:** ~$1,3 ΔΙΣ.

Στις 4 Δεκεμβρίου 2017 ένα phishing email έφτασε στη σλοβενική πλατφόρμα εξόρυξης **NiceHash**. Δύο μέρες αργότερα, Bitcoin αξίας **$75 εκατ.** είχαν φύγει — *«η μεγαλύτερη κλοπή στην ιστορία της Σλοβενίας»*, όπως το έθεσε ο υπεύθυνος προϊόντος. Η NiceHash αποζημίωσε κάθε πελάτη από τα μελλοντικά της κέρδη. Ήταν η αρχή μιας σειράς που, αποτιμημένη τη στιγμή κάθε κλοπής, έφτασε τα **$1,3 δισ.**

Τρεις τεχνικές εμφανίζονται εδώ που θα τις συναντήσεις και σήμερα, αναλλοίωτες. Η πρώτη είναι η **ψεύτικη εφαρμογή trading**: το Celas Trade Pro βγήκε τον Μάιο του 2018 με έναν καλοφτιαγμένο ιστότοπο που έδειχνε τα λογότυπα τεσσάρων εταιρειών antivirus με τις οποίες δεν είχε ποτέ μιλήσει. Το αρχείο ήταν πραγματικό λογισμικό με κακόβουλο κώδικα μέσα, στραμμένο στο πορτοφόλι σου. Η Kaspersky το αποκάλυψε, οπότε ξαναγύρισε ως WorldBit-Bot, μετά iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, JMT Trader, Dorusio, CryptoNeuro Trader και Ants2Whale — ίδια πλατφόρμα, νέο βάψιμο. Οι ερευνητές ονόμασαν την οικογένεια **AppleJeus**.

Η δεύτερη είναι η **ψεύτικη προσφορά εργασίας**. Οι ερευνητές βρήκαν την ομάδα να μελετά στόχους στο LinkedIn, να γράφει μια αγγελία στα μέτρα τους για θέση σε ανταγωνιστική εταιρεία, και να επισυνάπτει μια αίτηση που δήθεν προστατευόταν από τους ευρωπαϊκούς κανόνες προσωπικών δεδομένων και ζητούσε «enable content». Το κλικ εγκαθιστούσε backdoor. Η τρίτη είναι η **ψεύτικη εταιρεία**: η Marine Chain, μια εταιρεία tokenized ναυτιλίας που καταχωρήθηκε στο Χονγκ Κονγκ τον Απρίλιο του 2018, με αληθινούς επαγγελματίες και τέσσερα δικηγορικά γραφεία — αποκαλύφθηκε από έναν ανώνυμο χρήστη του Reddit, στη μοναδική ανάρτηση που έκανε ποτέ.

Η Δεύτερη Ματιά: τίποτα από αυτό το κεφάλαιο δεν έχει αποσυρθεί. Η ψεύτικη εφαρμογή έγινε ψεύτικος installer βιντεοκλήσης· η αγγελία του LinkedIn έγινε κακόβουλο αποθετήριο «τεχνικής δοκιμασίας». Η Chainalysis υπολογίζει τις κλοπές κρύπτο που αποδίδονται στη Β. Κορέα σε περίπου **$6,75 δισ.** από το 2016 — το $1,3 δισ. του White είναι πλέον κάτω από το ένα πέμπτο.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Κάθε εφαρμογή trading που κατεβάζεις είναι εχθρική μέχρι αποδείξεως του εναντίου.** Τα λογότυπα antivirus σε έναν ιστότοπο δεν αποδεικνύουν τίποτα.
2. **Μια απροσδόκητα τέλεια προσφορά εργασίας είναι μοτίβο επίθεσης.** Ειδικά αν έρχεται με αρχείο, repo ή installer.

> **Η ΟΥΣΙΑ**
>
> *Το εγχειρίδιο του 2018 δεν χρειάστηκε ποτέ αντικατάσταση. Μόνο καλύτερη παραγωγή.*

ΦΑΚΕΛΟΣ 07

Πάλι από την Αρχή

ATM σε είκοσι εννέα χώρες, ένας εκατομμυριούχος του Instagram, και γιατί οι εισαγγελείς απαγγέλλουν κατηγορίες σε ανθρώπους που δεν θα συλλάβουν ποτέ. Καλύπτει τα κεφάλαια 1 και 15.

ΣΤΟΧΟΙ: ΤΡΑΠΕΖΕΣ ΣΕ ΙΝΔΙΑ, ΠΑΚΙΣΤΑΝ, ΜΑΛΤΑ
ΕΤΗ: 2018–2019 · **ΚΛΑΠΗΚΑΝ:** ~$17ΕΚ

Στις 3 το μεσημέρι του Σαββάτου 11 Αυγούστου 2018, ένας ταξιτζής από τη Βομβάη, ένας φαρμακοποιός από την Πούνε και δεκάδες άλλοι σκόρπισαν στην ινδική πόλη Κολχαπούρ με στοίβες τραπεζικών καρτών. Στις 10 το βράδυ είχε τελειώσει. Παγκοσμίως, σε **είκοσι εννέα χώρες**, βγήκαν πάνω από **$11 εκατ.** από μηχανήματα σε **12.000 συναλλαγές** μέσα σε δύο ώρες και δεκατρία λεπτά. Οι μεταφορείς πληρώθηκαν έως $500 σε μια χώρα όπου ο μέσος ετήσιος μισθός είναι κάτω από $2.000. Η τράπεζα που είχαν σπάσει — η Cosmos Co-Operative — ήταν παραβιασμένη από τον Σεπτέμβριο του 2017. Δύο μήνες αργότερα το επανέλαβαν στην BankIslami του Πακιστάν για **$6,1 εκατ.**

Αυτό που κάνει τον φάκελο χρήσιμο είναι ποιους άλλους πιάνει. Οι κάρτες και το δίκτυο των μεταφορέων ήρθαν από τον **«Big Boss»** — τον Ghaleb Alaumary, Καναδό στο Οντάριο, που καταδικάστηκε σε έντεκα χρόνια και οκτώ μήνες. Επαφή του ήταν ο **Ramon Abbas**, «Hushpuppi», influencer του Instagram στο Ντουμπάι με 2,3 εκατομμύρια ακολούθους και διαμέρισμα στο Palazzo Versace. Μετά το χτύπημα στην Bank of Valletta τον Φεβρουάριο του 2019, όσοι ξέπλεναν το χρήμα πήγαν για ψώνια σε Harrods και Selfridges για Rolex, μια Jaguar και ένα Audi.

Οι Βορειοκορεάτες, ως συνήθως, δεν πιάστηκαν. Η απάντηση του White στο «γιατί να κατηγορήσεις κάποιον που δεν θα δικάσεις ποτέ» είναι η πιο πρακτική ιδέα του βιβλίου: το κατηγορητήριο είναι **εντολή κατεδάφισης**. Το 179σέλιδο κατηγορητήριο κατά του Park Jin Hyok κατέγραφε τους λογαριασμούς email του, τα προφίλ του, τους ιούς του και τις τακτικές του. Η δημοσίευση καίει την υποδομή και χτίζει συμμαχία θυμάτων.

Η Δεύτερη Ματιά: η στρατηγική άντεξε. Από το 2022 το FBI δημοσιεύει λίστες πορτοφολιών μέσα σε μέρες από κάθε μεγάλη κλοπή· πενήντα διευθύνσεις Ethereum δόθηκαν πέντε μέρες μετά το χτύπημα στην Bybit. Κανείς δεν περιμένει δίκη. Ο σκοπός είναι να γίνουν τα λεφτά δύσκολα στο ξόδεμα.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Το κράτος δίνει το χακάρισμα, το οργανωμένο έγκλημα τα χέρια.** Γι’ αυτό όσοι πιάνονται είναι σχεδόν πάντα οι ντόπιοι βοηθοί.
2. **Οι δημοσιευμένες λίστες πορτοφολιών είναι εργαλείο και για σένα.** Όταν ένα ανταλλακτήριο σημαδεύει διευθύνσεις, το σημάδι διαδίδεται.

> **Η ΟΥΣΙΑ**
>
> *Δεν μπορείς να τους συλλάβεις. Μπορείς να κάνεις τα λεφτά τους ραδιενεργά.*

ΦΑΚΕΛΟΣ 08

Όσα Δεν Πρόλαβε να Δει το Βιβλίο

Ο White έκλεισε το χειρόγραφο το 2021. Μετά, η ομάδα έγινε ο μεγαλύτερος κλέφτης κρύπτο στην ιστορία.

ΠΕΡΙΟΔΟΣ: 2022–2026 · **ΠΗΓΕΣ:** CHAINALYSIS, ELLIPTIC, TRM, FBI

Το τελικό σύνολο του βιβλίου ήταν $1,3 δισ. Η Chainalysis το ανεβάζει σήμερα σε περίπου **$6,75 δισ.** από το 2016, με **$2,02 δισ. μόνο το 2025**· η CertiK μετρά 263 περιστατικά.

ΗΜ/ΝΙΑ	ΣΤΟΧΟΣ	ΚΛΑΠΗΚΑΝ
Μαρ 2022	Ronin Bridge (Axie Infinity)	**~$620εκ**
Ιουν 2022	Harmony Horizon Bridge	**~$100εκ**
Ιουν 2023	Atomic Wallet	**>$100εκ**
Μαΐ 2024	DMM Bitcoin	**$308εκ**
Ιουλ 2024	WazirX	**$235εκ**
Φεβ 2025	Bybit	**~$1,5δισ**
Απρ 2026	Drift Protocol	**~$285εκ**
Απρ 2026	KelpDAO / rsETH bridge	**~$290εκ**

Η Bybit είναι αυτή που πρέπει να καταλάβεις. Στις 21 Φεβρουαρίου 2025 περίπου $1,5 δισ. σε ETH έφυγαν από το ανταλλακτήριο — που ποτέ δεν παραβιάστηκε. Ένας προγραμματιστής της Safe{Wallet}, του παρόχου multisig, παρασύρθηκε να τρέξει κακόβουλο project· από εκείνο το λάπτοπ άλλαξαν ένα αρχείο JavaScript με εκδοχή που ενεργοποιούνταν μόνο για το cold wallet της Bybit, και επανέφεραν το καθαρό δύο λεπτά μετά. Δεκαοκτώ μήνες αργότερα, η Bybit έχει ανακτήσει ή παγώσει περίπου **5%**.

Τι άλλαξε και τι όχι. Blender, Sinbad και eXch έκλεισαν και αντικαταστάθηκαν· αμερικανικό εφετείο ακύρωσε τις κυρώσεις στο Tornado Cash το 2024 και το μείγμα ακόμα χρησιμοποιείται. Το σταθερό μοτίβο είναι το σημείο εισόδου: όπως λέει η Elliptic, η αρχική παραβίαση είναι πλέον *συντριπτικά ανθρώπινη*.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Η επίθεση γίνεται πριν από σένα.** Οι χρήστες της Bybit δεν έκαναν τίποτα λάθος. Κρίνε μια πλατφόρμα από τη διαχείριση κλειδιών και τους προμηθευτές της.
2. **Τα ποσοστά ανάκτησης είναι τραγικά.** Ronin ~10%, Bybit ~5%. Η φύλαξη είναι ο έλεγχος· η ανάκτηση όχι.

> **Η ΟΥΣΙΑ**
>
> *Το βιβλίο τελειώνει στα $1,3 δισ. Το σύνολο είναι σήμερα πέντε φορές μεγαλύτερο — και η μέθοδος ίδια.*

ΦΑΚΕΛΟΣ 09

Η Προσφορά Εργασίας

Ο πιο πιθανός τρόπος με τον οποίο αυτή η ιστορία θα φτάσει σε σένα προσωπικά.

ΠΕΡΙΟΔΟΣ: 2022–2026 · **ΠΗΓΕΣ:** DOJ, MICROSOFT, UNIT 42, ESET

Το κεφάλαιο που ο White δεν έγραψε ποτέ τρέχει σε δύο κατευθύνσεις — και είναι το ίδιο πρόγραμμα. Στη μία, Βορειοκορεάτες *κάνουν αίτηση* για τη δουλειά σου. Στην άλλη, σου *προσφέρουν* μία.

Οι εργαζόμενοι. Η Multilateral Sanctions Monitoring Team — το σώμα που δημιουργήθηκε αφού η Ρωσία κατάργησε με βέτο την Ομάδα Εμπειρογνωμόνων του ΟΗΕ το 2024 — εκτιμά **1.000–2.000** Βορειοκορεάτες προγραμματιστές στο εξωτερικό σε τουλάχιστον οκτώ χώρες, με έσοδα **$350–800 εκατ. το 2024**, τα μισά περίπου από τα οποία στέλνονται πίσω. Χρησιμοποιούν κλεμμένες ταυτότητες, προφίλ γραμμένα με AI, και έναν συνεργάτη στις ΗΠΑ που φιλοξενεί το εταιρικό λάπτοπ σε «laptop farm», ώστε η σύνδεση να φαίνεται εγχώρια. Τον Ιούλιο του 2025 η Christina Chapman καταδικάστηκε σε 8,5 χρόνια για ένα τέτοιο: **309 αμερικανικές εταιρείες**, 68 κλεμμένες ταυτότητες, $17,1 εκατ. Τον Ιούνιο του 2025 τέσσερις Βορειοκορεάτες κατηγορήθηκαν ότι έκλεψαν $900.000 σε κρύπτο *από τους εργοδότες που τους προσέλαβαν*.

Οι προσφορές. Η Unit 42 της Palo Alto το ονόμασε **Contagious Interview**: ένας recruiter σε πλησιάζει στο LinkedIn ή στο Telegram, κανονίζεται τεχνική συνέντευξη, και κάποια στιγμή σου ζητούν να τρέξεις κάτι — κλώνησε αυτό το repo, εγκατέστησε αυτό το πακέτο, διόρθωσε την κάμερά σου επικολλώντας αυτή την εντολή. Τα φορτία (BeaverTail, InvisibleFerret, OtterCookie) κυνηγούν διαπιστευτήρια και δεκάδες επεκτάσεις πορτοφολιών. Η ESET βρήκε κακόβουλο κώδικα κρυμμένο σε σχόλια έξω από το ορατό παράθυρο του editor· η Kaspersky, προσεγγίσεις σε στελέχη και VC με *πραγματικά βίντεο προηγούμενων θυμάτων* και προθεσμία 30 λεπτών, για να μη σε αφήσουν να σκεφτείς.

Δεν είναι δευτερεύον κανάλι· είναι το κύριο. Η κλοπή $308 εκατ. από την DMM Bitcoin ξεκίνησε με ψεύτικο recruiter που έστειλε «τεστ πρόσληψης» σε Python σε υπάλληλο προμηθευτή λογισμικού πορτοφολιών.

ΤΙ ΣΗΜΑΙΝΕΙ ΓΙΑ ΣΕΝΑ

1. **Κάθε *npm install* από recruiter είναι εκτέλεση κώδικα στο μηχάνημά σου.** Γιατί ακριβώς αυτό είναι.
2. **Ποτέ μην τρέχεις τεστ συνέντευξης σε μηχάνημα με κλειδιά.** Ξεχωριστή συσκευή ή VM μιας χρήσης.
3. **Κανένας σοβαρός εργοδότης δεν σου ζητά να επικολλήσεις εντολή για να φτιάξεις την κάμερα.**

> **Η ΟΥΣΙΑ**
>
> *Το κράτος που λήστεψε κεντρική τράπεζα στέλνει τώρα προσφορές εργασίας.*

ΕΓΧΕΙΡΙΔΙΟ ΠΕΔΙΟΥ

Τι Σημαίνει για το Πορτοφόλι σου

Το πρακτικό υπόλοιπο δέκα φακέλων — για όσους κρατούν κρύπτο και δουλεύουν στην τεχνολογία.

ΚΟΙΝΟ: ΚΑΘΕ ΧΡΗΣΤΗΣ ΚΡΥΠΤΟ · **ΠΗΓΗ:** ΦΑΚΕΛΟΙ 00–09

Δεν είσαι κεντρική τράπεζα. Είσαι όμως μέσα στο στόχαστρο — γιατί το σημείο εισόδου σχεδόν σε κάθε υπόθεση αυτού του βιβλίου ήταν ένας απλός άνθρωπος με ένα inbox. Οι κανόνες που διδάσκουν οι φάκελοι:

1. **Ο recruiter είναι πλέον το μοντέλο απειλής** (φάκελοι 06, 09). Απρόσκλητη θέση, γενναιόδωρος μισθός, ένα repo ή installer στη διαδικασία. Επαλήθευσε την εταιρεία από τα δικά της επίσημα κανάλια, ποτέ από σύνδεσμο που σου δίνει ο «recruiter».
2. **Τα κλειδιά δεν αγγίζουν ποτέ μηχάνημα που τρέχει ξένο κώδικα** (φάκελοι 08, 09). Hardware wallet σε λάπτοπ όπου δοκιμάζεις repos αγνώστων δεν είναι cold storage.
3. **Ποτέ μην επικολλάς εντολή που δεν καταλαβαίνεις** (φάκελος 09). Σφάλματα κάμερας, «ενημερώσεις SDK», διορθώσεις drivers — το ψεύτικο σφάλμα *είναι* ο μηχανισμός παράδοσης.
4. **Κρίνε μια πλατφόρμα από τους προμηθευτές της** (φάκελος 08). Η Bybit έχασε $1,5 δισ. χωρίς να παραβιαστεί. Ρώτα ποιος υπογράφει και πόσοι.
5. **Υπόθεσε ότι η ανάκτηση είναι μηδέν** (φάκελοι 04, 08). Η Ronin επέστρεψε περίπου 10%, η Bybit περίπου 5%. Ό,τι δεν αντέχεις να χάσεις, κράτησέ το σε δική σου φύλαξη.
6. **Κάνε ενημερώσεις, και βάλ' τες αυτόματες** (φάκελος 05). Η διόρθωση του WannaCry ήταν μηνών.
7. **Κόψε ταχύτητα όταν κάποιος σου βάζει προθεσμία** (φάκελοι 02, 09). Τεστ 30 λεπτών, επείγουσες μεταφορές, προσφορές που λήγουν. Η κατασκευασμένη βιασύνη είναι το παλαιότερο εργαλείο και ακόμα το πιο αποτελεσματικό.
8. **Τα αντίγραφα ασφαλείας πρέπει να είναι offline** (φάκελοι 01, 05). Αν το αντίγραφό σου είναι προσβάσιμο από το μολυσμένο μηχάνημα, δεν έχεις αντίγραφο.

> **Η ΟΥΣΙΑ**
>
> *Ένα πυρηνικό κράτος χωρίς χρήματα αποφάσισε ότι το inbox σου είναι πηγή εσόδων. Φέρσου ανάλογα.*

Η ΕΤΥΜΗΓΟΡΙΑ

Το Βιβλίο στη Ζυγαριά

Κυκλοφόρησε το 2022 — βαθμολογημένο πάνω σε όσα ακολούθησαν.

ΣΥΓΓΡΑΦΕΑΣ: GEOFF WHITE, ΕΡΕΥΝΗΤΗΣ ΔΗΜΟΣΙΟΓΡΑΦΟΣ
ΒΑΘΜΟΣ: ΑΠΑΡΑΙΤΗΤΟ, ΜΕ ΕΝΑΝ ΑΣΤΕΡΙΣΚΟ

Η καλύτερη διαθέσιμη καταγραφή του πώς ένα κράτος μετατράπηκε σε εγκληματική επιχείρηση — και η μόνη που κρατά το βλέμμα της στους ανθρώπους που το πλήρωσαν. Ο πίνακας του σκορ:

- ✓ **Εξηγεί το κίνητρο, όχι μόνο τη μέθοδο** — ο λιμός, τα φαινόμενα καστάνιας, τα superdollars. Χωρίς αυτά τα κεφάλαια το χακάρισμα διαβάζεται ως κακία· μαζί τους διαβάζεται ως οικονομία.
- ✓ **Η κεντρική του προειδοποίηση γέρασε τέλεια** — ότι ο περιορισμός είναι το ξέπλυμα, όχι το χακάρισμα, και ότι η ομάδα μάθαινε να τον καταργεί. Όλα από το 2022 του δίνουν δίκιο.
- ✓ **Δίνει στα θύματα πραγματικές σελίδες** — η υπάλληλος της Sony που ζει ακόμα με εκτεθειμένο AMKA, τα λεφτά των αγροτών του Μπανγκλαντές, η ακυρωμένη εγχείρηση καρδιάς. Δημοσιογραφία, όχι θρίλερ.
- ✓ **Είναι ειλικρινές για την απόδοση ευθύνης** — μαζί με την προειδοποίηση του ίδιου του White ότι το «Park Jin Hyok» μπορεί να είναι κι αυτό το τελευταίο στρώμα της κούκλας.
- × **Το κομμάτι για τα κρύπτο είναι το πιο αδύναμο και το πιο ξεπερασμένο** — τελειώνει γύρω στο 2020, πριν από Ronin, DMM, Bybit και όλο το σχέδιο των «IT workers». Οι φάκελοι 08 και 09 υπάρχουν γι’ αυτό.
- × **Αφήνει τον αναγνώστη με επίγνωση, όχι με μέθοδο** — το τελικό κάλεσμα να είσαι «η τελευταία γραμμή άμυνας» είναι σωστό και ανεφάρμοστο. Δες το Εγχειρίδιο στην προηγούμενη σελίδα.

Τελικός βαθμός: ο απαραίτητος σύντροφος του *Tracers in the Dark*. Ο Greenberg έγραψε τους κυνηγούς· ο White τους κυνηγημένους. Διάβασε τον Greenberg για να μάθεις ότι το ledger καταδικάζει, και μετά τον White για να δεις ποιος χτίζει οικονομία από πάνω του έτσι κι αλλιώς. Αγόρασε το βιβλίο για τους φακέλους — έλα σε εμάς για τα πέντε χρόνια που δεν πρόλαβε.

> **Η ΟΥΣΙΑ**
>
> *Ο White κατέγραψε ένα συνεργείο ληστών τραπεζών. Από τότε που έκλεισε το χειρόγραφο, έγιναν ο μεγαλύτερος κλέφτης κρύπτο στην ιστορία.*