Χρήση λυτρολογισμικού (ransomware) εναντίον νοσοκομειακών συστημάτων

Κυριακή Θ. Διονυσοπούλου
Δικηγόρος Αθηνών

Προσφάτως, στο Düsseldorf της Γερμανίας σημειώθηκε κυβερνοεπίθεση κατά την διάρκεια της οποίας hackers, που εικάζεται ότι έδρασαν υποκινούμενοι από οικονομικά κίνητρα, κρυπτογράφησαν τα λογισμικά και ιατρικά δεδομένα ασθενών του πανεπιστημιακού νοσοκομείου της περιοχής. Με την εισβολή του λυτρολογισμικού σε 30 servers του νοσοκομείου, η διοίκησή του αναγκάστηκε να απομακρύνει ασθενείς που έχρηζαν επείγουσας ιατρικής περίθαλψης. Στόχος της επίθεσης ήταν η ψηφιακή οργάνωση του νοσοκομείου, η οποία συντόνιζε ιατρούς, θεραπείες, ακόμα και κλίνες. Το νοσοκομείο αναγκάστηκε να μειώσει δραστικά την χωρητικότητά του, αφού υπό φυσιολογικές συνθήκες θα μπορούσε να περιθάλψει τουλάχιστον 1.000 ασθενείς ημερησίως, αλλά εξαιτίας της επίθεσης δεν ήταν πλέον σε θέση να εξυπηρετήσει ούτε τους μισούς από αυτούς. Παράλληλα διέκοψε τις νέες εισαγωγές, προκειμένου να προστατευθούν όσοι είχαν ήδη εισαχθεί σε αυτό. Έτσι, μια γυναίκα, η οποία έπασχε από ανεύρυσμα κοιλιακής αορτής και βρισκόταν σε κρίσιμη κατάσταση, διακομίσθηκε σε νοσοκομείο της πόλης Wuppertal, 32 χιλιόμετρα μακριά και κατέληξε, δημιουργώντας προβληματισμό για το αν ο θάνατος της προήλθε από τις καθυστερήσεις στην ιατροφαρμακευτική της περίθαλψη, αφού το ασθενοφόρο εξαιτίας της κυβερνοεπίθεσης αναγκάστηκε να αλλάξει πορεία προς άλλο νοσοκομείο. Ο

θάνατός της χαρακτηρίστηκε ως ο πρώτος θάνατος που σημειώνεται από κυβερνοεπίθεση και εξ αυτού του λόγου συγκέντρωσε την παγκόσμια προσοχή.

Τα νοσοκομεία φαίνεται ότι αποτελούν συχνό στόχο των εν λόγω κυβερνοεπιθέσεων, αφού η επείγουσα ανάγκη πρόσβασης στα ιατρικά δεδομένα των ασθενών αυξάνει την πιθανότητα να υποκύψουν στον υλοποιούμενο εκβιασμό και να πληρώσουν τα λύτρα για την αποκρυπτογράφηση των λογισμικών τους συστημάτων. Μετά από επίθεση που εκδηλώθηκε σε μεγάλο νοσοκομείο των ΗΠΑ, νοσηλεύτριες ανέφεραν ότι κατά την διάρκεια του Σαββατοκύριακου, όταν ξεκίνησε η επίθεση στο νοσοκομείο όπου εργάζονταν, το ιατρικό προσωπικό κατέληξε να δουλεύει μόνο με στυλό και χαρτί. Ως εκ τούτου είναι προφανές ότι, για να εξασφαλίσουν μεγαλύτερη πιθανότητα επιτυχίας, οι hackers περιμένουν να εξαπολύσουν την επίθεσή τους κατά τις ημέρες που απασχολείται μειωμένος αριθμός τεχνικού προσωπικού στα νοσοκομεία, δηλαδή σε αργίες και Σαββατοκύριακα. Τα λύτρα δε που ζητούν κυμαίνονται από μερικές εκατοντάδες έως χιλιάδες δολάρια, πληρωτέα, φυσικά, σε bitcoin, τα οποία θεωρούνται ότι πυροδοτούν τέτοιου είδους επιθέσεις, αφού επιτρέπουν να γίνονται οι πληρωμές ανώνυμα.

Ήδη FBI[1], CISA[2] και HHS[3] ανακοίνωσαν ότι εν μέσω πανδημίας υπάρχει όχι μόνο υψηλός, αλλά και άμεσος κίνδυνος κυβερνοεπιθέσεων σε νοσοκομεία και παρόχους ιατρικής περίθαλψης. Βεβαίως, δεν είναι η πρώτη φορά που σημειώνεται τέτοιου είδους επίθεση κι ούτε η εν λόγω τακτική προήλθε από την πανδημική κατάσταση των νοσοκομείων: το 2017 οι επιθέσεις «WannaCry» και «NotPetya» πάγωσαν βρετανικά και αμερικανικά νοσοκομεία αντιστοίχως, αναγκάζοντας τα μεν πρώτα να ακυρώσουν προγραμματισμένα χειρουργεία, τα δε δεύτερα να αποδεσμεύσουν ασθενείς, στα ιατρικά δεδομένα των οποίων δεν είχαν πλέον πρόσβαση.

Προβληματισμοί δημιουργούνται αναφορικά με τις γενιές που καλούνται να εξοικειωθούν άμεσα με την δίκην κεραυνού εν αιθρία εισβολή των απλουστευμένων διαδικασιών της τεχνολογίας, που κάθε άλλο παρά προσιτές αποδεικνύεται ότι είναι, ειδικά σε μια χρονική περίοδο όπου όλα φαίνεται να αντικαθίστανται από νέους τεχνολογικούς τρόπους και συνήθειες. Σε κάθε περίπτωση, αυτό το πλέγμα νέων μορφών επικοινωνίας και πρόσβασης δημιουργεί νέα νομικά προβλήματα στα έως τώρα παραδοσιακά εγκλήματα, γεγονός που καταδεικνύει όχι μόνο την καλπάζουσα πραγματικότητα, αλλά και την ανάγκη συγχρονισμού της νομικής θεώρησης με τον ρου τον εξελίξεων. Η ασφάλεια στον κυβερνοχώρο είναι ένα μείζον ζήτημα σήμερα, αφού τέτοιους είδους επιθέσεις δεν περιορίζονται μόνο στην κρυπτογράφηση λογισμικού νοσοκομείων, αλλά και σε ή άλλες υπηρεσίες δημοσίου συμφέροντος, όπως πρόσφατα συνέβη με την μαζική εισβολή σε κυβερνητικές υπηρεσίες των ΗΠΑ.

1. Federal Bureau of Investigation.
2. Cybersecurity and Infrastructure Security Agency.
3. Department of Health and Human Services.

Τέτοιου είδους περιστατικά κυβερνοεπιθέσεων συνδέονται αναμφισβήτητα με μια νέα γενιά εγκληματικής συμπεριφοράς, η οποία, πέραν της ευθύνης του δράστη για παρακώλυση λειτουργίας πληροφοριακών συστημάτων (άρ. 292Β ΠΚ), γεννά ποινικά ζητήματα που αφορούν αφενός το πεδίο της εκβίασης και αφετέρου το πεδίο της ανθρωποκτονίας εκ προθέσεως. Μέχρι πρότινος ανάλογες μορφές συμπεριφοράς είχαν απασχολήσει την ποινική θεωρία και πράξη σε σχέση με παρόμοιες επιθέσεις που εκδήλωναν δράστες ευρισκόμενοι στην αλλοδαπή, οι οποίοι κρυπτογραφούσαν τα δεδομένα ηλεκτρονικών υπολογιστών ιδιωτών της ημεδαπής (χρησιμοποιώντας μάλιστα απατηλά μέσα: π.χ. κατά το πάγωμα της οθόνης του ηλεκτρονικού υπολογιστή εμφάνιζαν στον χρήστη λογότυπο της αστυνομίας, συνοδεύοντας το με εκφοβιστικό μήνυμα που αφορούσε την αξιόποινη δράση του, λ.χ. παράνομο κατέβασμα ταινίας) και ακολούθως απαιτούσαν την καταβολή χρηματικού ποσού ύψους συνήθως 100 € ως λύτρα για την επαναφορά του υπολογιστή στην προτέρα κατάσταση.

Δεν χωρεί καμία αμφιβολία ότι οι εν λόγω κυβερνοεπιθέσεις εγείρουν ζήτημα ποινικής ευθύνης για τετελεσμένη ή εν αποπείρα εκβίαση, η οποία διαπράττεται μέσω απειλής παράλειψης μιας ενέργειας που ο δράστης έχει ιδιαίτερη νομική υποχρέωση να τελέσει εξαιτίας της προγενέστερης επικίνδυνης και άδικης συμπεριφοράς του, δηλαδή της κρυπτογράφησης των δεδομένων του θύματος. Μάλιστα, εφόσον η παράλειψη του δράστη ενδέχεται να έχει ως συνέπεια τον θάνατο ενός ή περισσοτέρων ασθενών που λόγω της επιθέσεως δεν μπορούν πλέον να τύχουν της δέουσας ιατρικής αντιμετώπισης, το εδώ περιγραφόμενο περιστατικό δύναται να ενταχθεί στο πεδίο της (κακουργηματικής) ληστρικής εκβιάσεως, η αντικειμενική υπόσταση της οποίας προϋποθέτει απειλή ενωμένη με επικείμενο κίνδυνο σώματος ή ζωής (άρ. 380 παρ. 1 β΄ ΠΚ).

Περαιτέρω, τίθεται το ζήτημα της ευθύνης για ανθρωποκτονία εκ προθέσεως του δράστη μιας επιθέσεως με χρήση λυτρολογισμικού εναντίον νοσοκομειακών μονάδων, όταν ως χρόνος τέλεσης της επίθεσης έχουν επιλεγεί ημέρες, κατά τις οποίες η λειτουργία των νοσοκομείων γίνεται με μειωμένο τεχνικό προσωπικό, κάτι που έχει ως συνέπεια να μην μπορεί να αντιμετωπιστεί εγκαίρως ένα επείγον περιστατικό και να αποβιώσουν ευρισκόμενοι σε κρίσιμη κατάσταση ασθενείς. Πολύ δύσκολα θα μπορούσε να υποστηριχθεί πειστικά ότι ένας δράστης που εκδηλώνει μια τόσο επικίνδυνη επίθεση σε βάρος νοσοκομειακής μονάδας δεν αναλογίστηκε το ενδεχόμενο ότι θα κοστίσει η επίμαχη ενέργειά του τη ζωή ενός ή περισσότερων ασθενών, οι οποίοι δεν θα μπορούσαν να λάβουν έγκαιρη ιατρική φροντίδα, απαραίτητη για την αντιμετώπιση της κρίσιμης κατάστασης της υγείας τους. Αλλά ακόμη κι αν είχε περάσει από το μυαλό του το ενδεχόμενο αυτό, θα ήταν εξίσου δύσκολο να υποστηρίξει πειστικά ότι πίστευε βασίμως στην μη επέλευση του θανατηφόρου αποτελέσματος. Αυτός είναι και ο λόγος για τον οποίον δεν θα ήταν ορθή η αξιολόγηση του εξεταζόμενου περιστατικού υπό το πρίσμα της θανατηφόρας εκθέσεως, αφού η ύπαρξη ενδεχόμενου δόλου, όπως εν προκειμένω, ως προς την επέλευση του βαρύτερου αποτελέσματος, δηλαδή του θανάτου, οδηγεί στην εφαρμογή της αρχής της απορρόφησης κατ' εφαρμογήν των κανόνων της συρροής: η θανατηφόρα έκθεση θα απορροφηθεί από το βαρύτερο έγκλημα της ανθρωποκτονίας

εκ προθέσεως. Φυσικά, ζήτημα ευθύνης του δράστη θα μπορούσε να τεθεί και για τόσες απόπειρες ανθρωποκτονίας όσοι ήταν οι ασθενείς, η ζωή των οποίων κινδύνευσε.

Πάντως, η μέχρι τώρα αδυναμία επίλυσης βασικών δογματικών προβλημάτων σχετικά με την ύπαρξη ή μη του ενδεχόμενου δόλου δεν ευνοεί την σχετική συζήτηση με αφορμή τις νέες αυτές μορφές εγκληματικής συμπεριφοράς. Πολλώ δε μάλλον, σε περιπτώσεις, όπως η προκείμενη, όπου ο κίνδυνος για τους ασθενείς εναπόκειται στην διακριτική ευχέρεια των hackers και έως το σημείο που επιθυμούν εκείνοι να φτάσουν. Εν προκειμένω, οι hackers απεκάλυψαν το κλειδί αποκρυπτογράφησης των δεδομένων όταν πληροφορήθηκαν ότι με την επίθεση τους χτύπησαν νοσοκομειακή μονάδα. Πρέπει δε να τονιστεί ότι η εν λόγω κίνηση εκ μέρους των δραστών, σύμφωνα με τον Markus Hartmann, επικεφαλής της εισαγγελίας της Κολωνίας, προήλθε από τις μεγάλες διαστάσεις δημοσιότητας που έλαβε το εν λόγω γεγονός, καθώς η μέχρι τώρα εμπειρία τους σε τέτοιου είδους επιθέσεις καταδεικνύει ότι οι hackers κάνουν τα πάντα χάριν του οικονομικού οφέλους. Διάλογο ως προς τον αιτιώδη σύνδεσμο στην προκειμένη περίπτωση έχει ανοίξει η κρίσιμη κατάσταση της ασθενούς, αφού αφενός δύναται να στοιχειοθετηθεί ο αιτιώδης σύνδεσμος ανάμεσα στην πράξη της κυβερνοεπίθεσης και του θανάτου της εάν αποδειχθεί ότι η ασθενής κατέληξε ακόμη και λίγες ώρες νωρίτερα από ότι θα κατέληγε, αφετέρου η μη στοιχειοθέτηση του αιτιώδους συνδέσμου αφήνει μόνο περιθώριο στις αρχές να χρησιμοποιήσουν τις παραδοσιακές κατηγορίες περί εκβίασης, εάν φυσικά καταφέρουν να εντοπίσουν τους δράστες.

Μόνο κατά το περσινό έτος δέχτηκαν επίθεση 750 πάροχοι ιατρικής περίθαλψης στις ΗΠΑ και όπως υποστηρίζεται είναι θέμα χρόνου να θρηνήσουμε θύματα από τις εν λόγω επιθέσεις. Άλλωστε, όπως ήδη τονίστηκε, η ιδιαίτερη κατάσταση της πανδημίας έχει καταστήσει τα νοσοκομεία στόχο των επίδοξων δραστών, αλλά σε κάθε περίπτωση ο κίνδυνος είναι ήδη εν γένει υψηλός, αφού μόλις πριν από λίγο καιρό τεράστια κυβερνοεπίθεση σημειώθηκε σε ομοσπονδιακές υπηρεσίες και μεγάλες εταιρείες των ΗΠΑ. Οι επιθέσεις σήμερα έχουν αλλάξει μορφή και η ολοένα αυξανόμενη απειλή των κυβερνοεπιθέσεων δημιουργεί μεγάλη ανησυχία σε ό,τι αφορά ειδικά τους τομείς της υγείας, αφού η ανάγκη νομοθετικών ρυθμίσεων είναι όχι μόνο εμφανής αλλά και αναγκαία, ενώ ακόμα δεν έχει βρεθεί αποτελεσματικός τρόπος αντίδρασης για την αντιμετώπιση τους.

ΠΗΓΕΣ

- https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html?fbclid=IwAR03SCho_KilINZUnsYwz1yFsygPDIlOczKvvdaP7pvXRYuVCRP1GE97djA
- https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are
- https://www.wired.co.uk/article/ransomware-hospital-death-germany
- https://fortune.com/2020/09/23/cyberattack-death-dusseldorf-germany-ransomeware-ambulance/
- https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254
- https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi
- https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html