https://oaskhths.blogspot.com/2020/11/h-darktrace-cybereason.html

Η Darktrace, η Cybereason και η Τεχνολογική Μοναδικότητα της Αυτοσυνείδητης Τεχνητής Νοημοσύνης

Αναρτήθηκε από Ασκητής Νοεμβρίου 06, 2020

Darktrace και Cybereason: Οι εταιρείες- βιτρίνα των μυστικών υπηρεσιών που επιδιώκουν να εξουσιάσουν τον κόσμο με την AI Singularity (την Τεχνολογική Μοναδικότητα της Αυτοσυνείδητης Τεχνητής Νοημοσύνης)

Του Τζόνι Βέντμορ

Όλοι ονειρευόμασταν, ένα όνειρο όπου μπορούσατε να επιπλεύσετε ή να γλιστρήσετε στον ονειρόκοσμο σας χωρίς κόπο. Αυτό προκαλεί ένα αίσθημα τρόμου, σαν να έχετε την ικανότητα να αφεθείτε, και αν αφεθείτε είτε θα πετάξετε είτε θα γκρεμιστείτε.

Βρισκόμαστε τώρα σε ένα σημείο της Ιστορίας όπου είτε τα επερχόμενα γεγονότα θα μελετούνται για χιλιάδες χρόνια, είτε θα τα θυμόμαστε ως το σημείο όπου χάσαμε εντελώς την ανθρώπινη κατάσταση μας. Η τεχνολογία της τεχνητής νοημοσύνης (AI) έχει εισέλθει σε μια νέα φάση τα τελευταία χρόνια, όπου αντί οι αλγόριθμοι τεχνητής νοημοσύνης να μαθαίνουν από τον άνθρωπο, τώρα διδάσκονται μόνοι τους και αλλάζουν τους δικούς τους αλγόριθμους καθώς μαθαίνουν. Βρισκόμαστε στο κατώφλι του να αφήσουμε τον έλεγχο εντελώς, τόσο σύντομα, λόγω μερικών μικρών εταιρειών που τους έχει δοθεί σιωπηλά η ελεύθερη εξουσία με πρόσχημα την «προστασία» της ψηφιακής μας ζωής, και όλα αυτά μέσα σε έναν τεχνολογικό τομέα που

κινείται τόσο γρήγορα που δεν μπορούμε πλέον να δούμε τι ακολουθεί αμέσως μετά.

Όλος ο ελεύθερα σκεπτόμενος πληθυσμός της Γης θα ήθελε λίγο περισσότερο χρόνο για να συζητήσει μια τέτοια κοσμογονική αλλαγή. Ωστόσο, οι τεχνοκράτες και οι επιστήμονες, υποστηριζόμενοι από τους επιχειρηματίες, ήδη εφαρμόζουν το μέλλον, προτού οι μάζες βρουν την ευκαιρία ακόμα και να σκεφθούν τις συνέπειές. Με ελάχιστη νομοθεσία να διέπει τις τεχνολογίες τεχνητής νοημοσύνης, οι κυβερνήσεις μας είναι πρόθυμες να βάλουν κάθε πρωτοπόρο της τεχνολογίας να κάνει εφευρέσεις, ενώ δεν υπάρχει απόδοση ευθυνών για τυχόν ζημιές που προκύπτουν. Δεν μιλάμε για μια μεγάλη κοινωνική αναστάτωση, μιλάμε για το πιθανό γεγονός της εξαφάνισης της δικής μας δημιουργίας. Αντί να κάνουμε προσεκτικά μικρά βήματα αντιθέτως περιμένουμε να πετάξουμε απλώς με το να αφεθούμε.

Πρόκειται να βιώσουμε μια μνημειώδη αλλαγή στην τεχνολογία, ξεκινώντας με την κυβερνοασφάλεια "επόμενης γενιάς" η οποία θα προχωρήσει γρήγορα προς στο άγνωστο. Η ανεπιτήρητη τεχνητή νοημοσύνη, που τώρα «τρέχει» σε κρίσιμα δίκτυα σε όλο τον κόσμο ως προϊόν «κυβερνοασφάλειας», εξελίσσει τον ίδιο της τον αλγόριθμο χωρίς την ανάγκη συμμετοχής των ανθρώπων. Εν τω μεταξύ, οι πλούσιοι χορηγοί αυτής της μελλοντικής τεχνολογίας αιχμής έχουν εφορμήσει και εργάζονται για να ωθήσουν τις κοινωνίες μας σε αυτό το νέο, ανεξερεύνητο και δυστοπικό τεχνολογικό όριο.

Αλλά ποιες είναι οι αυτές οι εταιρείες τις οποίες χρηματοδοτούν αυτοί οι πρόθυμοι πλούσιοι επιχειρηματίες, για να δημιουργήσουν ένα αυτόνομο άνευ προηγουμένου, κυβερνητικό σύστημα άμυνας βασισμένο στην τεχνολογία της τεχνητής νοημοσύνης; Είναι πράγματι εταιρείες αν αναλογιστούμε τις βαθιές και άμεσες σχέσεις τους με τις υπηρεσίες πληροφοριών; Μήπως θα έπρεπε αυτές οι εταιρείες να επανακατηγοριοποιηθούν ως απλές προεκτάσεις των κρατικών υπηρεσιών πληροφοριών που λειτουργούν χωρίς τους περιορισμούς απόδοσης δημόσιων ευθυνών;

Κάθε μία από αυτές τις εταιρείες έχει δημιουργηθεί από ομάδες πρώην πρακτόρων μυστικών υπηρεσιών, μερικοί εκ των οποίων βρέθηκαν στα υψηλότερα κλιμάκια των μυστικών υπηρεσιών των χωρών τους. Και η MI5 και η CIA έχουν σημαντικό ρόλο σε αυτές τις καταχθόνιες επιχειρήσεις, αλλά **η Μονάδα 8200 του Ισραήλ είναι η κύρια ομάδα που αξιοποιεί αυτήν την πρόοδο των ανεπιτήρητων αλγορίθμων τεχνητής νοημοσύνης οι οποίοι είναι ικανοί να αλλάξουν τον κόσμο (σ.ι. σύντομα και στην Ανατολική Ιερουσαλήμ).**

Ωστόσο, αυτές οι ίδιες οι εταιρείες φαίνεται να πωλούν αμυντικά συστήματα ενάντια σε έναν πιθανό Αρμαγεδδώνα τον οποίο μπορεί οι ίδιες να προκαλέσουν. Έχουν τις λύσεις για τα κυβερνοπροβλήματα όλων ή τουλάχιστον αυτή είναι η εικόνα που θέλουν να παρουσιάσουν. Επιτρέψτε μου να σας συστήσω τις πιο επικίνδυνες επιχειρήσεις πληροφοριών στον πλανήτη Γη, οι οποίες μεταμφιέζονται ως εταιρείες κυβερνο-ασφάλειας.

Darktrace - Η ανεπιτήρητη εταιρεία κυβερνο-ασφάλειας βάσει αλγορίθμων μηχανικής μάθησης

Τα μέλη της Darktrace δεν κρύβουν τους στόχους τους. Μιλάνε για τα δημοσίως αποθηκευμένα δεδομένα σαν να έχουν ήδη το δικαίωμα να τα πωλήσουν σε οποιονδήποτε ανά τον κόσμο. **Τα δεδομένα είναι το καύσιμο της Τέταρτης Βιομηχανικής Επανάστασης** και η Darktrace έχει βγάλει σχεδόν 2 δισεκατομμύρια δολάρια στην αγορά των δεδομένων κατά τη διάρκεια της σχετικά σύντομης ιστορίας της, φτάνοντας σε κατάσταση Unicorn με μεγάλη ευκολία. Όταν η Darktrace δημιούργησε για πρώτη φορά τον ιστότοπό της το 2013, η περιγραφή του οράματος της τιτλοφορούνταν ως: «Η νέα κανονικότητα: Μάθετε την ανθρώπινη και την μηχανική συμπεριφορά για να μειώσετε τους κινδύνους της κυβερνο-ασφάλειας». Τότε ήμασταν λιγότερο εξοικειωμένοι με τον όρο «νέα κανονικότητα», αλλά τώρα βρίσκεται παντού ολόγυρα μας. Η Darktrace ήδη δραστηριοποιείται στο Εθνικό Σύστημα Υγείας του Ηνωμένου Βασιλείου (NHS), το ηλεκτρικό δίκτυο του Ηνωμένου Βασιλείου, και σε πολλά άλλα σημαντικά σημεία κρίσιμων υποδομών της Βρετανίας και επεκτείνεται γρήγορα σε όλο τον κόσμο (σ.ι. Για Ελλάδα και Κύπρο βλ. εδώ).

Ο Ντέιβ Πάλμερ ήταν αντιτρομοκρατικός πράκτορας της MI5 και εργαζόταν στους Ολυμπιακούς Αγώνες του Λονδίνου το 2012, όταν αυτός και μερικοί από τους συναδέλφους του είχαν για πρώτη φορά την αρχική ιδέα για αυτό που μετά εξελίχθηκε στην Darktrace. Ήθελαν να δημιουργήσουν ένα σύστημα κυβερνο-ασφάλειας βασισμένο στο ανθρώπινο ανοσοποιητικό σύστημα, ένα σύστημα διαφορετικό από τα παραδοσιακά antivirus. Αυτό το σύστημα θα αναζητούσε ανωμαλίες στις διαδικασίες ενός υπολογιστικού δικτύου ώστε να

στοχεύσει σε ένα ευρύτερο φάσμα πιο περίπλοκων ζητημάτων στον κυβερνοχώρο.

Ο Palmer είχε περάσει 14 χρόνια δουλεύοντας για την MI5 και τη GCHQ στη δημιουργία ασφαλών δικτύων επικοινωνίας για τους Βρετανούς κατασκόπους. Τελικά στα τέλη του 2012 προσέγγισε δύο μαθηματικούς από το Πανεπιστήμιο του Κέιμπριτζ για να τον βοηθήσουν στην πραγματοποίηση του ονείρου του. Αυτοί οι μαθηματικοί εργάζονταν σε πρότζεκτς σχετικά με τη χρήση ανεπιτήρητης μηχανικής μάθησης για να διδάξουν έναν υπολογιστή να έχει αίσθηση του εαυτού του, ένα βήμα που θα έφερνε μια τέτοια τεχνολογία επικίνδυνα κοντά στη λεγόμενη τεχνολογική μοναδικότητα. Σε αυτό το σημείο, όπως προειδοποίησαν τόσο οι κριτικοί όσο και οι υποστηρικτές της αυτοσυνείδητης τεχνητής νοημοσύνης, η μηχανική νοημοσύνη όχι μόνο θα ξεπεράσει την ανθρώπινη νοημοσύνη, αλλά θα προχωρήσει με έναν ακατανόητο ρυθμό, επιφέροντας τεράστιες και παγκόσμιες επιπτώσεις.

Σε μια ομιλία στο TechCrunch του 2016, η τότε προσφάτως διορισμένη συν-διευθύνουσα σύμβουλος της Darktrace, Poppy Gustafsson , πιάστηκε στα πράσα προσπαθώντας να παραπλανήσει το κοινό σχετικά με την προέλευση της εταιρείας. Χρησιμοποίησε το βήμα του TechCrunch για να ισχυριστεί ότι η «σπίθα» για τη δημιουργία της Darktrace προήλθε αρχικά από τους μαθηματικούς του Cambridge και υποβάθμισε τη συμμετοχή των μυστικών υπηρεσιών όπως η MI5, η GCHQ και η CIA. Η συντονίστρια του TechCrunch η Νατάσα Λόμας, επέδειξε εξαίρετη δημοσιογραφική ακεραιότητα σε εκείνη την περίσταση και ζήτησε διευκρινίσεις :«Δηλαδή, πρώτα έγινε η έρευνα των μαθηματικών και μετά μπλεχτήκατε μαζί με τους κατασκόπους; Τι έγινε πρώτα; » ρώτησε η ατρόμητη Λόμας. Η Gustafsson στριφογύρισε ελαφρώς σε άβολη θέση και είπε: «Έγινε ακριβώς έτσι. Αρχικά ήταν η μηχανική μάθηση που μιλούσε για το πώς θα αναλύσει έναν υπολογιστή για να τον βοηθήσει να κατανοήσει τον εαυτό του. Και μετά ήταν οι, χμμ, εμπειρογνώμονες από τις κυβερνητικές υπηρεσίες πληροφοριών που σκέφτηκαν «ωχ, αυτό θα μπορούσε να εφαρμοστεί στο πρόβλημα ασφάλειας του κυβερνοχώρου». «Αλλά αυτή η δήλωση ήταν ένα εξώφθαλμο ψέμα και η Gustafsson δεν είναι και η πιο ταλαντούχα ψεύτρα.

Η Gustafsson, η οποία ήταν αρχικά CFO και COO της νεοσύστατης Darktrace, διευθύνει την εταιρεία μαζί με την άλλη συν-διευθύνουσα σύμβουλο Nicole Eagen, απόφοιτο της Oracle, μιας μεγάλης τεχνολογικής εταιρείας που επίσης προέρχεται από τις υπηρεσίες πληροφοριών. Και τα δύο μέλη του γυναικείου ντουέτου της Darktrace μετακινήθηκαν από την Invoke Capital, από τον αρχικό επενδυτή και μέλος του διοικητικού συμβουλίου της Darktrace, τον δισεκατομμυριούχο Dr. Mike Lynch OBE από το Ηνωμένο Βασιλείο. Ο Δρ Mike Lynch θεωρείται ένας από τους πιο σημαντικούς επενδυτές στον τομέα της τεχνολογίας και περιγράφει τον εαυτό του ως «την απάντηση του Ηνωμένου Βασιλείου στον Μπιλ Γκέιτς». Οι προηγούμενες επιτυχημένες προσπάθειές του ήταν με την Autonomy, μια εταιρεία τεχνολογίας που έχει εμπλέξει τον Lynch σε μια νομική διαμάχη με την HP σχετικά με τον δόλιο πληθωρισμό της αξίας της και την Blinkx, μια εταιρεία αναζήτησης βίντεο από της οποίας το διοικητικό συμβούλιο αναγκάστηκε αργότερα να παραιτηθεί.

Τα προβλήματα του Δρ Mike Lynch με την Hewlett Packard δεν πρέπει να υποτιμούνται, όπως έγινε σαφές σε ένα άρθρο της Telegraph όπου αυτά τα προβλήματα περιγράφηκαν ως «η δίκη του αιώνα». Όμως, ο Mike Lynch πρέπει πρώτα να εκδοθεί και η παρατεταμένη δικαστική του διαμάχη για να αποφύγει την έκδοση οδήγησε σε κάποια αβεβαιότητα σχετικά με το μέλλον της Darktrace όσο ο Lynch εξακολουθεί να έχει ενεργό ρόλο εντός της εταιρείας. Πρόσφατα αναφέρθηκε επίσης στα ΜΜΕ ότι η τράπεζα της Wall Street , η Goldman Sachs αρνήθηκε να αναλάβει ρόλο στην αρχική δημόσια προσφορά (IPO) της Darktrace λόγω της συνεχιζόμενης διαμάχης για την έκδοση του Mike Lynch.

Ωστόσο, η Darktrace δεν αποτελείται μόνο από έναν άνθρωπο. Η εταιρεία υπερηφανεύεται ότι πάνω από 4000 οργανισμοί παγκοσμίως βασίζονται πλέον στις τεχνολογίες τεχνητής νοημοσύνης της. Με έδρα το Σαν Φρανσίσκο των ΗΠΑ και το Cambridge του Ηνωμένου Βασιλείου, η Darktrace απασχολεί περισσότερους από 1300 υπαλλήλους σε 44 χώρες και ο αριθμός τους αυξάνεται. Και παρόλο που οι διασυνδέσεις της με τις κρατικές υπηρεσίες πληροφοριών είναι σαφείς και προφανείς, η Darktrace είναι επίσημα μια εντελώς ιδιωτική επιχείρηση με μεγάλους επενδυτές, συμπεριλαμβανομένων των KKR, Summit Partners, Vitruvian Partners, Samsung Ventures, TenEleven Ventures, Hoxton Ventures, Talis Capital, Invoke Capital και Insight Venture. Μαζί με τον αμφιλεγόμενο Δρ. Mike Lynch OBE, στο διοικητικό συμβούλιο της Darktrace βρίσκονται μερικοί άνθρωποι με μεγάλη επιρροή οι οποίοι συνδέονται στενά με τις μυστικές υπηρεσίες των ΗΠΑ και του Ηνωμένου Βασιλείου

Ένα από τα πρώτα μέλη που διορίστηκαν στο διοικητικό συμβούλιο της Darktrace ήταν ο Jonathan Evans, γνωστός επίσης ως βαρώνος Evans του Weardale. Ο Evans ήταν προηγουμένως Γενικός Διευθυντής της MI5, ανέλαβε από την Dame Eliza Manningham-Buller το 2007 και έμεινε στην ανώτατη θέση των μυστικών υπηρεσιών του Ηνωμένου Βασιλείου έως το 2013. Μετά τη θητεία του ως επικεφαλής της MI5, ο Evans εντάχθηκε αρχικά στην HSBC Holdings ως μη εκτελεστικός διευθυντής, έναν ρόλο που ανέλαβε επίσης και στην Ark, ένα εξαιρετικά ασφαλές κέντρο δεδομένων στο Ηνωμένο Βασίλειο.

Εάν παρευρισκόσασταν σε μια συνεδρίαση του διοικητικού συμβουλίου της Darktrace, θα μπορούσατε να πιστέψετε ότι παρευρίσκεστε πραγματικά σε μια συνάντηση του Υπουργείου Εσωτερικών του Ηνωμένου Βασιλείου από το παρελθόν. Η πρώην υπουργός Εσωτερικών Amber Rudd επί πρωθυπουργίας Theresa May, έγινε μέλος της Darktrace μετά το τέλος της κυβερνητικής θητείας της το 2019. Είναι επίσης στο ΔΣ της Teneo, μιας συμβουλευτικής εταιρείας που συνιδρύθηκε και διευθύνεται από τον Doug Band, πρώην σύμβουλο του Bill Clinton και στενό φίλο του διαβόητου Jeffrey Epstein. Όπως πάντα, όταν ερευνάται ο σκοτεινός κόσμος των μυστικών υπηρεσιών πληροφοριών, αποκαλύπτονται πολλές διασυνδέσεις με τον Epstein και την συνεργάτιδα του Ghislaine Maxwell.

Μια που τους αναφέραμε, ένα άλλο μέλος του ΔΣ της Darktrace επίσης συνδέεται με τον Epstein και την Maxwell. Ο αφοσιωμένος στην CIA, Alan Wade, είναι ένα από τα πιο ενδιαφέροντα μέλη του ΔΣ της Darktrace.

Ανακοινώθηκε στις 10 Μαΐου 2016 ότι διορίζεται στο ΔΣ της και στο παρελθόν υπήρξε πρώην προϊστάμενος πληροφοριών της CIA. Τα τριάντα πέντε χρόνια της καριέρας του στα κορυφαία κλιμάκια της CIA έληξαν το 2006 και στη συνέχεια αφιέρωσε το χρόνο του για να βοηθήσει εταιρείες του ιδιωτικού τομέα συνδεδεμένες με την CIA .

Ενώ υπηρετούσε σε μια κορυφαία θέση των μυστικών υπηρεσιών των ΗΠΑ, ο Wade ίδρυσε τη Chiliad μαζί με την αδερφή της Ghislaine Maxwell, την Christine Maxwell. Όπως ανέφερε το Unlimited Hangout νωρίτερα αυτό το έτος, η Christine Maxwell συμμετείχε προσωπικά στην ηγεσία των επιχειρήσεων της εταιρείας-βιτρίνας που χρησιμοποιούσε ο πατέρας της Robert Maxwell για την εμπορία του λογισμικού PROMIS τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα των ΗΠΑ, το οποίο είχε backdoor για τις ισραηλινές μυστικές υπηρεσίες. Δεδομένου του ιστορικού της, το ότι ο Wade επέλεξε από όλους τους ανθρώπους να συνιδρύσει μια μεγάλη εταιρεία λογισμικού με την Christine Maxwell λέει σίγουρα πολλά.

Όταν ήταν ακόμη εν ενεργεία, η Chiliad αυτοπροσδιοριζόταν ως «ηγετική εταιρεία στην ανάλυση δεδομένων μεταξύ clouds, υπηρεσιών, τμημάτων και άλλων εστιών» και έτρεχε στους υπολογιστές και τις βάσεις δεδομένων σχεδόν κάθε μεγάλου συστήματος εθνικής ασφάλειας της κυβέρνησης των ΗΠΑ. Σήμερα όμως, ο ανενεργός ιστότοπος της δείχνει μόνο το τυπικό μήνυμα σφάλματος.

Ολοκληρώνουμε με το ΔΣ της Darktrace με τον κατ' όνομα ακαδημαϊκό τους, τον καθηγητή Nick Jennings CB FREng, ο οποίος υπηρετεί ως ερευνητικός και επιχειρηματικός αντιπρύτανης στο Imperial College του Λονδίνου. Ωστόσο, ο Jennings υπήρξε επίσης επικεφαλής επιστημονικός σύμβουλος Εθνικής Ασφαλείας της κυβέρνησης του Ηνωμένου Βασιλείου και σήμερα είναι μέλος του συμβουλίου τεχνητής νοημοσύνης της κυβέρνησης του Ηνωμένου Βασιλείου, μια πολύ βολική θέση δεδομένων των φιλοδοξιών της Darktrace.

Όλοι αυτοί που ηγούνται της Darktrace και του ΔΣ της είναι έτοιμοι να προτείνουν μια λύση σε όλα μας τα προβλήματα που σχετίζονται με την κυβερνοασφάλεια. Μπορείτε απλά να εγκαταστήσετε ένα κουτί και να αφήσετε τη Darktrace να φροντίσει το δίκτυό σας, και να εμπιστευτείτε μια τεχνητή νοημοσύνη που κοντεύει να γίνει αυτόνομη και την οποία διαχειρίζονται άτομα που σχετίζονται με τις μυστικές υπηρεσίες με αμφιλεγόμενο παρελθόν, όλα αυτά για την «ευκολία» και για να έχετε την ησυχία σας. Αλλά τι θα πολεμούν ακριβώς;

Cybereason - Από επιθετικοί χάκερς που χρηματοδοτούνται από το κράτος, στην κυβερνοασφάλεια της τεχνητής νοημοσύνης

κλικ στην εικόνα

Όπως έχουμε βιώσει σε άλλες αξέχαστες στιγμές της ιστορίας, οι συμπτωματικές προσομοιώσεις πριν από ή κατά τη διάρκεια οποιουδήποτε χειραγωγημένου γεγονότος από τις μυστικές υπηρεσίες, είναι συνηθισμένες. Σε αυτήν την περίπτωση, μια εταιρεία με την επωνυμία Cybereason μας επιτρέπει να ρίξουμε μια ματιά στο επερχόμενο φοβερό μέλλον. Σε πολλές προσομοιώσεις που η Cybereason έχει κάνει τα τελευταία χρόνια, εξετάζει πώς πιθανές κυβερνοεπιθέσεις θα μπορούσαν να προκαλέσουν αδιανόητη καταστροφή στις εκλογές των ΗΠΑ του 2020.

Ο διευθύνων σύμβουλος και συνιδρυτής της Cybereason είναι ένας αινιγματικός πρώην μυστικός πράκτορας του Ισραήλ, ο Lior Div-Cohen, που συχνά αναφέρεται ως Lior Div. Ο Div που του έχει απονεμηθεί το Μετάλλιο της Τιμής του ισραηλινού στρατού και είναι πρώην μέλος της Ισραηλινής Μονάδας 8200, ίδρυσε την Cybereason το 2012 μαζί με τους Yossi Naar και Yonatan Striem-Amit, οι οποίοι είναι επίσης βετεράνοι της στρατιωτικής κυβερνοασφάλειας του Ισραήλ. Ο Lior Div αποφοίτησε από το Ακαδημαϊκό Κολλέγιο του Τελ Αβίβ, στη συνέχεια εργάστηκε ως μηχανικός λογισμικού για την Xacct, έναν πάροχο υπηρεσιών δικτύου, και στη συνέχεια στη διαβόητη εταιρεία Amdocs, η οποία κατηγορήθηκε για υποκλοπές εναντίον αμερικανών κυβερνητικών αξιωματούχων για λογαριασμό του Ισραήλ. Μετά την Amdocs και πριν την Cybereason, ο Lior Div ήταν Διευθύνων Σύμβουλος και συνιδρυτής της Ισραηλινής εταιρείας κυβερνοασφάλειας AlfaTech, η οποία περιγράφεται στα ισραηλινά ΜΜΕ ως «Μια εταιρεία υπηρεσιών κυβερνοασφάλειας για τις ισραηλινές κυβερνητικές υπηρεσίες».

Η Cybereason, σε μια παράξενη διαφήμιση που προωθούσε ένα ανύπαρκτο προϊόν ονόματι Cyberblast , περιέγραψε εαυτόν ως «ηγέτιδα στην προστασία τελικού σημείου, που προσφέρει ανίχνευση και απόκριση τελικού σημείου, antivirus επόμενης γενιάς και διαχειριζόμενες υπηρεσίες παρακολούθησης που υποστηρίζονται από πρωτοπόρο, στρατιωτική τεχνολογία, αξιοποιώντας την τεχνητή νοημοσύνη και την μηχανική μάθηση». Οι υπεύθυνοι μάρκετινγκ της Cybereason τα δώσαν όλα για να παρουσιάσουν εαυτούς ως μια start-up

τύπου Silicon Valley όπου περνούν όλες τις μέρες τους μαγειρεύοντας, πίνοντας, χορεύοντας και μη κάνοντας σχεδόν τίποτε, αλλά στην πραγματικότητα είναι μια εταιρεία που ανήκει εν μέρει στον αμυντικό κολοσσό Lockheed Martin και έχει πολύ στενούς δεσμούς με τις ισραηλινές υπηρεσίες πληροφοριών. Μέσω της συνεργασίας της με την Lockheed Martin, πλέον το λογισμικό κυβερνοασφάλειας της Cybereason που βασίζεται στην τεχνητή νοημοσύνη,«τρέχει» σε μερικά από τα πιο απόρρητα δίκτυα της αμερικανικής κυβέρνησης, συμπεριλαμβανομένων πολλών, κρίσιμων στρατιωτικών συστημάτων των ΗΠΑ.

Ωστόσο, δεν είναι μόνο οι μεγάλες κατασκευάστριες όπλων όπως η Lockheed Martin που έχουν επενδύσει σε αυτήν την πλατφόρμα υψηλής τεχνολογίας στον κυβερνοχώρο. Το Reuters ανέφερε τον Αύγουστο του 2019 ότι η ιαπωνική εταιρεία Softbank έχει επενδύσει προηγουμένως στην εταιρεία, μαζί με τις εταιρείες venture capital CRV και Spark Capital. Το επενδυτικό χαρτοφυλάκιο της Spark Capital περιλαμβάνει τις εταιρείες Twitter, Oculus, Wayfair, Coinbase, Plaid, μεταξύ πολλών άλλων μεγάλων παικτών. Οι επενδύσεις της CRV περιλαμβάνουν τις εταιρείες Dropbox, Patreon, αλλά και εταιρείες σχετιζόμενες με την τεχνητή νοημοσύνη και την μηχανικη μάθηση, όπως η Standard Cognition και η Dyno Therapeutics.

Όπως και η Darktrace, η Cybereason προσφέρει αυτό που περιγράφεται ως τεχνολογία antivirus επόμενης γενιάς, η οποία αντί να ανταποκρίνεται σε επιθέσεις όταν εντοπίζονται, χρησιμοποιεί τεχνητή νοημοσύνη και μηχανική μάθηση για να βλέπει ανωμαλίες στις συνήθεις διαδικασίες ενός δικτύου, σε πραγματικό χρόνο.

Μερικές από τις προσομοιώσεις που διενήργησε η Cybereason τα τελευταία δύο χρόνια μας οδηγούν στην ημέρα των εκλογών. Σε ένα βίντεο με τίτλο: 2018 -10 Χακάροντας την ψήφο από ένα σενάριο και μια προσομοίωση με τίτλο Blackout:Προστατέψτε την ψηφοφορία, η προσομοίωση εξέτασε ποια τμήματα των διαδικασιών της ημέρας των εκλογών ήταν ευάλωτα στους χάκερ. Ξεκαθάρισαν από την αρχή ότι δεν αφορά μόνο τα μηχανήματα ψηφοφορίας.

Επιχείρηση Blackout

Η Nolandia, η φανταστική πόλη της Επιχείρησης Blackout, βασίστηκε σε μια μέση αμερικανική πόλη. Στη Nolandia, τρεις ομάδες χάκερς θα ανταγωνίζονταν μεταξύ τους για τον έλεγχο της πόλης.

Οι τρείς ομάδες και οι ρόλοι τους συνοπτικά σύμφωνα με τους Ross Rustici και Sam Curry της Cybereason ήταν:

Red Team AKA Broken Eagle Task Force: Ο βασικός στόχος της Broken EagleTask Force ήταν να διαταράξει τις εκλογικές διαδικασίες σε πραγματικό χρόνο. Η προσέγγιση αυτής της ομάδας εξελίχθηκε καθ 'όλη τη διάρκεια της προσομοίωσης προκαλώντας όσο το δυνατόν μεγαλύτερη, ζημιά κάνοντας το αποτέλεσμα των εκλογών όσο το δυνατόν περισσότερο αμφισβητίσημο και

πολιτικά προκατειλημμένο Επιχείρησαν να ελέγξουν το αφήγημα ότι το σύστημα είχε διαλυθεί και ότι οι εκλογές δεν ήταν αξιόπιστες.

Blue Team AKA Nolandia Event Task Force: Οι Blue κατά βάση αντιδρούσαν κατά τη διάρκεια της προσομοίωσης και βρίσκονταν συνεχώς ένα βήμα πίσω. Η ομάδα Blue, ανταποκρινόμενη σε μια κλήση για διαρροή φυσικού αερίου σε ένα εκλογικό τμήμα της Nolandia στις αρχές της προσομοίωσης, επικοινώνησε με το γραφείο του Υπουργού Εξωτερικών για να ρωτήσει εάν πρέπει να κλείσουν το εκλογικό τμήμα. Ευτυχώς, το πραγματικό υπουργείο Εξωτερικών είχε δύο συμβούλους που συμμετείχαν στην προσομοίωση οι οποίοι ήταν σε θέση να προσφέρουν εναλλακτικά σχέδια έκτακτης ανάγκης διαθέσιμα στον πραγματικό κόσμο στην Αμερική. Μέχρι το τέλος της προσομοίωσης, οι Blue γνώριζαν ότι είχαν αποτύχει σε μεγάλο βαθμό στην άσκηση.

White Team AKA White Control Team: Αυτή η ομάδα λειτούργησε υποστηρικτικά δίνοντας συμβουλές ή την άδεια στις δύο ομάδες. Ο κύριος στόχος αυτής της ομάδας ήταν να εξισορροπήσει τον ρεαλισμό του σεναρίου και να δημιουργήσει προβλήματα για κάθε ομάδα που θα βίωναν στον πραγματικό κόσμο.

Τον Νοέμβριο του 2019, η Cybereason επανέλαβε την προσομοίωση επίθεσης κατά την ημέρα των εκλογών σε μια εκδήλωση στην Ουάσιγκτον και έχει εκτελέσει πολλές προσομοιώσεις τον τελευταίο χρόνο.Η τελευταία φανταστική αμερικανική πόλη ονομάστηκε Adversaria. Ενώ η ημέρα των εκλογών πλησιάζει όλο και περισσότερο, η Cybereason δημοσιεύει διαδικτυακά τα καλύτερα προωθητικά βίντεο.Εάν ήσασταν προσεκτικοί τότε θα έχετε παρατηρήσει ότι η Cybereason πέρασε όλο τον Οκτώβριο του 2020 διαφημιζόμενη σε μεγάλο βαθμό καθώς πλησιάζει η μεγάλη μέρα τους. Εκπρόσωποι της Cybereason αναφέρονται σε κάθε ιστορία τρόμου στα ΜΜΕ

Το Vice News δημοσίευσε ένα άρθρο στις 7 Οκτωβρίου με τίτλο: «Τα νοσοκομεία έχουν γίνει «πρωταρχικοί στόχοι» για διαδικτυακές επιθέσεις Ransomware,» όπου αναφέρουν τον Ισραήλ Μπαράκ, τον επικεφαλής αξιωματικό ασφαλείας της Cybereason. Το άρθρο αναφέρει ότι ο Μπαράκ είναι ο «ειδικός κυβερνοπολέμου της Cybereason, όπου πέρασε εννέα χρόνια στις Ισραηλινές Αμυντικές Δυνάμεις ως ειδικός στα αμυντικά συστήματα στον κυβερνοχώρο». Και όταν στο ρεπορτάζ του Adam Scroxton στο Computer Weekly στις 20 Οκτωβρίου, αναφέρθηκε η καταδίκη των έξι υποτιθέμενων Ρώσων χάκερ της διάσημης επίθεσης NotPetya, η Cybereason μέσω του CSO της, Sam Curry, έκανε δηλώσεις.

Σε ένα πεντάλεπτο βίντεο του καναλιού Freethink στις 21 Οκτωβρίου 2020, με τίτλο Hacker's Simulate Election Day Blackout , ο Sam Curry, Διευθύνων Σύμβουλος Ασφαλείας της Cybereason, μιλά ανοιχτά για τις πιθανότητες παρεμβολής στην ημέρα των εκλογών κατά την επερχόμενη Προεδρική αναμέτρηση. «Κανείς δεν έχει δει μια εκλογική αναμέτρηση όπως αναμένουμε να είναι οι Προεδρικές Εκλογές του 2020», λέει ο Curry, «τα στοιχήματα είναι υψηλά για το 2020. Ειλικρινά, αυτό είναι το παιχνίδι που πρέπει να κερδηθεί».

Σε ένα άρθρο του Wired στις 22 Οκτωβρίου με τίτλο «Οι 12 κυβερνο-απειλές που θα μπορούσαν να προκαλέσουν καταστροφή στις εκλογές» αναφέρεται: «Η εταιρεία ασφάλειας Cybereason πέρυσι πραγματοποίησε μια σειρά επιτραπέζιων ασκήσεων που εξετάζουν συγκεκριμένα πώς πραγματικές επιθέσεις μπορούν να επηρεάσουν την ημέρα των εκλογών. Μια άσκηση που επικεντρώθηκε σε μια hacktivist ομάδα - γνωστή στην άσκηση ως "Kill Organized Systems (K-OS)", χάκαρε τους φωτεινούς οδικούς σηματοδότες και σταμάτησε τις εκλογές παραλύοντας τις αστικές μεταφορές της πόλης». Η Cybereason δεν έχει εμφανιστεί ποτέ τόσο πολύ στα ΜΜΕ όσο εμφανίστηκε τον περασμένο Οκτώβριο. Θα μπορούσε ακόμη κανείς να υποθέσει ότι αυτές οι εμφανίσεις είναι μια μιντιακή καμπάνια που οδηγεί σε ένα μεγάλο γεγονός.

Και στη συνέχεια, στις 26 Οκτωβρίου 2020, η Cybereason κυκλοφόρησε ένα νέο προωθητικό βίντεο με τίτλο: «Είμαστε οι υπερασπιστές. Οι πρώτοι στον αγώνα σας». Στο δίλεπτο βίντεο, ένας αφηγητής με χολιγουντιανό ύφος συνοδεύεται από μια CGI κουκουβάγια ρομπότ-δολοφόνο, με μαχαίρια αντί για φτερά και λαμπερά μάτια γεμάτια κακία. Προφανώς προσπαθούν να προβάλουν την εικόνα ενός από τους σοφούς και παλιούς προστάτες του κυβερνοχώρου... ή ίσως κάτι πολύ χειρότερο. Η Cybereason είναι αρκετά απειλητική και χωρίς τις κουκουβάγιες ρομπότ-δολοφόνους.

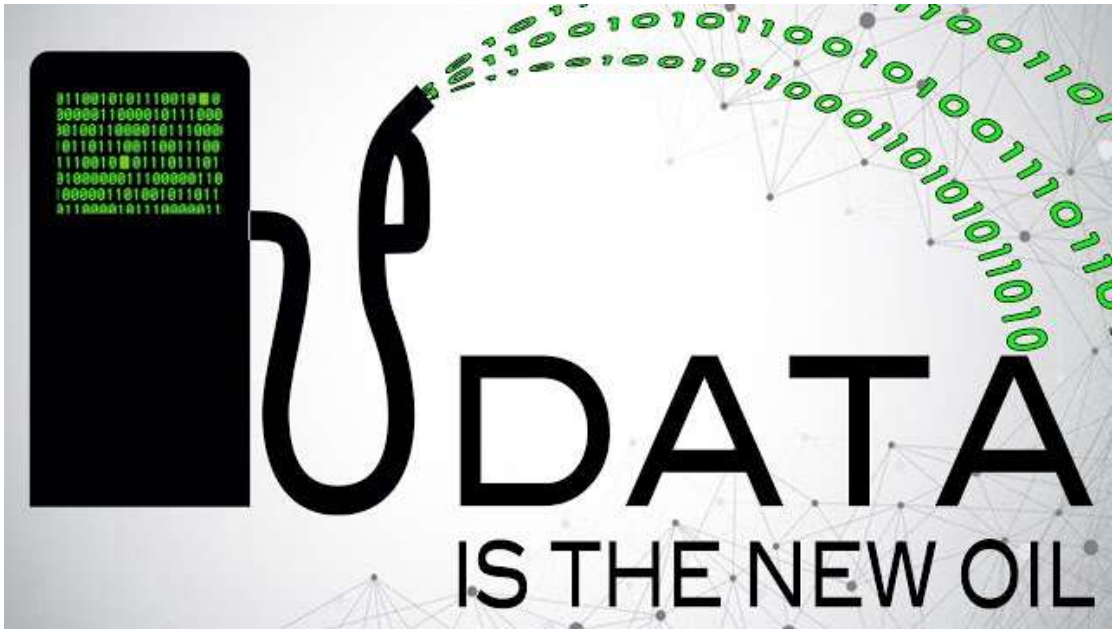
Οι συνήθεις ύποπτοι

Η Cybereason έχει επίσης διασυνδέσεις με έναν από τους συνήθεις υπόπτους, τον ταξίαρχο Pinchas Buchris. Είναι πρώην Αναπληρωτής Διοικητής μιας ελίτ μονάδας επιχειρήσεων του Ισραηλινου Στρατού και πρώην Διοικητής της στρατιωτικής Μονάδας 8200 Cyber Intelligence Unit. Διετέλεσε επίσης Γενικός Διευθυντής του Ισραηλινού Υπουργείου Άμυνας, Διευθύνων Σύμβουλος της Oil Refineries Ltd και επίσης υπηρετεί ως μέλος του διοικητικού συμβουλίου της AIPAC. Αυτός ο μεγαλόσχημος ισραηλινός μυστικός πράκτορας προσχώρησε στο διοικητικό συμβούλιο της Cybereason λίγο μετά την θητεία του στην Carbyne911. Η Carbyne, μια ισραηλινή πλατφόρμα κλήσεων άμεσης ανάγκης (911) που είχε αρχικούς επενδυτές τους Jeffrey Epstein, Nicole Junkermann και Peter Thiel, ιδρύθηκε από τον Ehud Barak και άλλους πρώην μεγάλους πράκτορες του Ισραήλ.

Η Carbyne911 είναι ένα εξαιρετικό παράδειγμα για το πώς οι ισραηλινές εταιρείες πληροφοριών προσπαθούν να ανατρέψουν και να διεισδύσουν στα τρέχοντα συστήματά μας. Και από το αρχικό μου άρθρο του 2019 όπου αποκάλυψα την απειλητική ομάδα των πρώην μελών της Μονάδας 8200, η Carbyne άλλαξε σχεδόν όλα τα μέλη του διοικητικού συμβουλίου της. Τώρα, τα μέλη που επιλέχτηκαν στο διοικητικό συμβούλιο είναι σχεδόν όλοι πρώην Αμερικανοί πράκτορες και κρατικοί εκπρόσωποι χωρίς κανέναν από τη Μονάδα 8200. Αυτή ήταν μια προφανής προσπάθεια να απομακρυνθεί η εταιρεία από τις ισραηλινές μυστικές υπηρεσίες και να προχωρήσει προς τον στόχο τους που είναι ο έλεγχος των ιδιωτικών δεδομένων κάθε Αμερικανού. Η Carbyne911 πιέζει να συμμετάσχει στις εφαρμογές ιχνηλάτησης του Covid-19

και συνεχίζει να προσπαθεί να αναλάβει την αμερικανική επικοινωνιακή υποδομή των γραμμών έκτακτης ανάγκης. Οι άνθρωποι της Carbyne911 θα εξεταστούν λεπτομερέστερα μια άλλη μέρα.

Οι εταιρείες Darktrace, Cybereason και Carbyne911 δεν είναι απλώς πρωτοπόρες σε έναν κλάδο τεχνολογίας που κινείται γρήγορα. Αντιθέτως, συνδέονται εγγενώς με τις κλασσικές υπηρεσίες πληροφοριών που προσπαθούν να επαναπροσδιοριστούν με ένα διαφορετικό, πιο αποδεκτό προκάλυμμα. **Δημιουργούν την υποδομή που έχει σχεδιαστεί για να ανατρέψει τα τρέχοντα συστήματά μας. Μια ανεπιτήρητη τεχνητή νοημοσύνη που θα απαιτεί όσο το δυνατόν περισσότερα δεδομένα για να τροφοδοτείται και οι κυβερνήσεις μας έχουν ήδη συμφωνήσει να δώσουν ό, τι μπορούν.**



Όλες αυτές οι τεχνολογίες πρέπει να μελετηθούν, όχι μόνο σε σχέση με μια κυβερνοεπίθεση ή ένα τρομοκρατικό συμβάν την ημέρα των εκλογών, αλλά αντιθέτως να μελετηθούν **εντός του αρχικού και ευρύτερου πλαισίου**. **Οι μαθηματικοί του Κέιμπριτζ πίσω από τη δημιουργία της Darktrace δεν σκέφτονταν να αποτρέψουν μια κυβερνοεπίθεση την ημέρα των εκλογών το 2020. Αυτοί οι μεγαλοφυείς μαθηματικοί προσπαθούσαν να δημιουργήσουν την τεχνολογική μοναδικότητα, τη δημιουργία αυτόνομης αυτοδιδασκόμενης τεχνητής νοημοσύνης. Αυτή η προηγμένη τεχνολογία θα τροφοδοτείται σύντομα με περισσότερα σύνολα δεδομένων από όσα ο ανθρώπινος εγκέφαλος μπορεί να φανταστεί. Σε μια κίνηση να συνδεθεί η αυτόνομη τεχνητή νοημοσύνη online, οι κυβερνοαπειλές για τις εκλογές θα είναι απλώς ένα προπέτασμα καπνού για να αποφευχθούν τα μεγαλύτερα και πιο συναφή ζητήματα της δημόσιας πολιτικής σχετικά με την ασφάλεια και την ηθική της ανεπιτήρητης αυτόνομης αυτοδιδασκόμενης τεχνητής**

νοημοσύνης , και το πιο σημαντικό, οι μεγάλοι κίνδυνοι που σχετίζονται με αυτά τα άγνωστα συστήματα.

Οι εταιρείες που κατέχουν αυτήν την πανίσχυρη μελλοντική τεχνολογία δεν αποκρύπτουν καν τις διασυνδέσεις και τις συμμαχίες τους. Οι διάφορες εταιρείες τους είναι γεμάτες Αμερικανούς, Βρετανούς και Ισραηλινούς πράκτορες πληροφοριών που σχεδιάζουν να χρησιμοποιήσουν αυτό το είδος τεχνολογίας για να στοχεύσουν τους δικούς τους πληθυσμούς (σ.ι. Και όχι μόνο) . Δεν είναι τυχαίο λοιπόν ότι μερικά από αυτά τα έθνη εργάζονται κρυφά για την ανάπτυξη μιας τεχνητής νοημοσύνης που θα αντικαταστήσει τους ανθρώπους χάκερ, αυτοματοποιώντας την ίδια την απειλή από την οποία εταιρείες όπως η Darktrace και η Cybereason ισχυρίζονται ότι μας προστατεύουν.