Η επίθεση στο GitHub φώτισε το έργο της AKAMAI

28 Φεβρουαρίου 2018, μεταξύ 17:21 και 17:30 UTC

Το traffic του GitHub, μιας πλατφόρμας που χρησιμοποιούν εκατομμύρια developers σε όλον τον κόσμο, κορυφώνεται στα 1,35 terabits per second

28 Φεβρουαρίου 2018, 17:21 UTC

Το σύστημα ελέγχου της GitHub αντιλαμβάνεται την απειλή και ειδοποιεί τους μηχανικούς ασφαλείας

28 Φεβρουαρίου 2018, 17:26 UTC

Τα συστήματα της AKAMAI λαμβάνουν την εντολή να τραβήξουν πάνω τους το traffic του GitHub

28 Φεβρουαρίου 2018, 17:30 UTC

Το GitHub είναι ξανά λειτουργικό μέσα σε 9 και μόνο λεπτά της ώρας

Κάπως έτσι εξελίχθηκε το περιστατικό της μεγαλύτερης μέχρι τώρα DDoS επίθεσης, με τη δεύτερη μεγαλύτερη να έχει συμβεί στα τέλη του 2016, κάνοντας ένα peak traffic στα 1,2 terabits per second.

Σε αντίθεση με άλλες επιθέσεις που χρειάζονται μολυσμένους υπολογιστές για να πραγματοποιηθούν, αυτές οι δύο βασίστηκαν στην εκμετάλλευση των κενών ασφαλείας των memcached servers, οι οποίοι υπολογίζονται περίπου στους 100.000 σε όλον τον κόσμο. Ο επιτιθέμενος αναλαμβάνει τον έλεγχο των servers, οι οποίοι συχνά δεν έχουν ούτε κωδικό εισόδου και τους ζητά να στείλουν τεράστιες ποσότητες δεδομένων σε μια συγκεκριμένη διεύθυνση. Δεδομένου ότι την περασμένη εβδομάδα συνέβη ένας καταιγισμός επιθέσεων αυτού του τύπου, με μικρότερη ένταση από αυτήν που χτύπησε το GitHub, οι προμηθευτές των εν λόγω servers έχουν ξεκινήσει να στέλνουν ειδοποιήσεις στους κατόχους τους, ώστε να φροντίσουν για την βελτίωση της ασφάλειας τους. Ωστόσο, οι αναλυτές ασφαλείας θεωρούν πολύ πιθανό χιλιάδες από αυτούς τους servers να παραμείνουν ευάλωτοι .Ο Dale Drew, chief security strategist της εταιρείας CenturyLink, δήλωσε ότι το τελευταίο διάστημα περίπου 300 διαφορετικοί ανιχνευτές αναζητούσαν memcached servers, το οποίο σημαίνει ότι υπάρχουν τουλάχιστον 300 διαφορετικά άτομα ή ομάδες ατόμων που ενδιαφέρονται για εκτεθειμένους servers.

Ποιος ήταν ο ρόλος της AKAMAI

Η υπηρεσία Prolexic της AKAMAI λειτουργεί σαν κόσκινο. Όταν αναλάβει τον έλεγχο δέχεται το σύνολο του εισερχόμενου και εξερχόμενου traffic και αφού ξεφορτώσει τα "σκουπίδια" επιστρέφει στην κυκλοφορία τα χρήσιμα δεδομένα.

Ο Josh Shaul, vice president του τμήματος web security της AKAMAI δήλωσε λίγο μετά την επίθεση ότι "η εταιρεία είχε προετοιμαστεί σε θεωρητικό επίπεδο για ένα τέτοιο συμβάν και προσδοκούσε ότι σε ένα πραγματικό περιστατικό θα μπορούσε να ανταποκριθεί άψογα, κάτι που τελικά συνέβη."

Μάλιστα, όπως έγινε γνωστό, η AKAMAI είχε πρόσφατα θωρακίσει την υπηρεσία της, ειδικά για επιθέσεις που θα μπορούσαν να γίνουν από memcached servers.

Γιατί όμως οι επιτιθέμενοι να εκθέσουν τα όπλα τους;

Μπορεί η επίθεση στο GitHub να ήταν εντυπωσιακή, αλλά τελικά ολοκληρώθηκε χωρίς απώλειες ή ζημίες. Από μια άλλη οπτική, αυτή καθώς και άλλες παρόμοιες επιθέσεις έχουν εκθέσει πλέον το κενό ασφαλείας των memcached servers και θα οδηγήσουν στην καλύτερη προστασία τους. Ακόμα και αν η επίθεση ήταν πετυχημένη δεν θα υπήρχε εμπορική ζημιά για το GitHub, δεδομένου ότι δεν είναι εμπορική υπηρεσία. Με την πρώτη ματιά, η πράξη ακούγεται άσκοπη. Εκτός και αν θεωρήσουμε ότι οι ειδικοί ασφαλείας έχουν δίκιο και τελικά παρά το συμβάν χιλιάδες memcached servers θα συνεχίσουν να παραμένουν εκτεθειμένοι.

Τελικά, το μεγαλύτερο όφελος προέκυψε για την AKAMAI, η οποία μπόρεσε να αποδείξει πρώτα στην ίδια και στη συνέχεια στους εν δυνάμει πελάτες της ότι είναι έτοιμη να αντέξει επιθέσεις τέτοιου βελνεκούς, αλλά και ακόμα μεγαλύτερες, καθώς όπως αναφέρει εκπρόσωπος της, η υποδομή της είναι προετοιμασμένη για να αντέξει πολλαπλάσια μεγαλύτερες συγχρονισμένες επιθέσεις σε σχέση με αυτή που δέχτηκε το GitHub. **NW**

Η ΕΛΛΑΔΑ ΣΤΟ ΕΠΙΚΕΝΤΡΟ ΤΩΝ **DDOS ΕΠΙΘΕΣΕΩΝ**

Είναι πολλά αυτά για τα οποία η Ελλάδα βρίσκεται στο επίκεντρο τα τελευταία χρόνια και ένα εξ αυτών είναι και οι κυβερνοεπιθέσεις σε ιδιωτικούς και κυβερνητικούς οργανισμούς. Όσα δημοσιεύονται στα μέσα μαζικής ενημέρωσης είναι ένα μόνο κλάσμα των επιτυχημένων επιθέσεων, το οποίο με τη σειρά του είναι κλάσμα των επιθέσεων που αποτράπηκαν.
Ο ρόλος της AKAMAI εστιάζει, μεταξύ άλλων στην αποτροπή των επιθέσεων και ο τρόπος που το επιτυγχάνει ήταν το αντικείμενο της συζήτησης μας με τον Αντώνη Μαυρομιχάλη, AKAMAI Business Unit Director στην ATCOM. Η ATCOM αποτελεί τον επίσημο reseller των υπηρεσιών της AKAMAI στην Ελλάδα (silver status reseller), ενώ το συγκεκριμένο Business Unit της εταιρείας προσφέρει στην αγορά υψηλής ποιότητας υπηρεσίες ασφαλείας, web performance και διανομής διαδικτυακού περιεχομένου.

Ποια είναι τα όπλα της AKAMAI απέναντι στο κυβερνοέγκλημα;
Με περισσότερους από 250.000 servers σε όλον τον κόσμο, οι οποίοι συστεγάζονται σε υποδομές παρόχων Internet, έχουμε τη δυνατότητα να ελέγχουμε σχεδόν το 30% του traffic σε παγκόσμιο επίπεδο. Επομένως, μπορούμε να δούμε μια κυβερνοεπίθεση τη στιγμή της γέννησης της και ανάλογα με την υπηρεσία που έχει αγοράσει ο πελάτης, να γίνει σε αυτόν από ελάχιστα ως καθόλου αισθητή. Στην περίπτωση της GitHub για παράδειγμα, η υπηρεσία είναι on demand, οπότε ο πελάτης εντόπισε με δικό του προσωπικό ασφαλείας την επίθεση και από τη στιγμή που μας ενημέρωσε εμείς την είχαμε αποσβέσει σε χρόνο λιγότερο από 5 λεπτά, όπως προβλέπει η σύμβαση που έχουμε υπογράψει. Αυτό που κάνουμε είναι ότι με τη βοήθεια ενός αλγορίθμου που γεννήθηκε πριν την ίδρυση της εταιρείας στα εργαστήρια του MIT, κατανέμουμε το φορτίο της επίθεσης σε servers που λειτουργούν ως φίλτρα ή ως σκουπιδότοποι. Αν ο πελάτης έχει αγοράσει κάποια Always On υπηρεσία, τότε δε χρειάζεται καν να αντιληφθεί την επίθεση. Η σύμβαση που έχει υπογράψει τον καλύπτει με 100% προστασία και άρα πρακτικά 0% downtime των συστημάτων του.

Έτσι όπως μας περιγράφετε τις υπηρεσίες, θεωρητικά θα έπρεπε να μην υπάρχουν εταιρείες που δεν είναι πελάτες σας
Στην πράξη συμβαίνει κάτι τέτοιο, αλλά λόγω συμβολαίων εμπιστευτικότητας δεν έχουμε τη δυνατότητα να αποκαλύπτουμε τα ονόματα των πελατών μας. Μόλις 18 μήνες μετά την έναρξη λειτουργίας του, το AKAMAI Business Unit της ATCOM περιλαμβάνει στο πελατολόγιο του εταιρείες και οργανισμούς από διαφορετικούς κλάδους όπως, ενδεικτικά, ο τραπεζικός - χρηματοοικονομικός, οι τηλεπικοινωνίες, το λιανεμπόριο και τα Μέσα Ενημέρωσης. Υποστηρίζει τα περισσότερα high traffic και e-commerce websites της χώρας, προσφέροντας εκτός των security services που αναφέρθηκαν, την πλήρη γκάμα παρεχόμενων υπηρεσιών content delivery & web performance της AKAMAI.

Είναι ο κίνδυνος για την Ελλάδα εξίσου σημαντικός με άλλες μεγαλύτερες αγορές;
Το τελευταίο διάστημα, η Ελλάδα φαίνεται να έχει μπει στο στόχαστρο. Καθημερινά, τα συστήματα μας αποσβένουν περισσότερες από μια επιθέσεις, όχι βέβαια της έντασης του GitHub, αλλά αρκετά δυνατές ώστε να βγάλουν εκτός λειτουργίας τα συστήματα ενός οργανισμού. Ωστόσο, οι υπηρεσίες μας δεν εστιάζουν μόνο στον τομέα της ασφάλειας. Διαθέτουμε και υπηρεσίες, οι οποίες βοηθούν εταιρείες με εμπορικά site να προσφέρουν με ταχύτητα τα εμπορεύματά τους και τις υπηρεσίες τους. Δεδομένης της αύξησης στη χρήση του Internet στην Ελλάδα, αρκετά πλέον site επιβαρύνονται με μεγάλα φορτία κίνησης και ειδικά σε περιόδους αιχμής, όπως είναι οι εορταστικές.

Θα μπορούσε μια εταιρεία με κέρδη μερικών χιλιάδων ευρώ να αξιοποιήσει τις υπηρεσίες σας;
Η AKAMAI διαθέτει πλέον προϊόντα που απευθύνονται σε όλα τα μεγέθη των εταιρειών. Επίσης θα ήθελα να τονίσω την αξία που έχουν κάποιες από τις υπηρεσίες της στις νέες απαιτήσεις που θέτει ο κανονισμός GDPR. Θεωρητικά, η αξιοποίηση των συστημάτων μας θα μπορούσε να προσφέρει πολύ υψηλό ποσοστό ασφάλειας απέναντι σε μια επίθεση που έχει στόχο την κλοπή δεδομένων και άρα να μειώσει το ρίσκο της επιχείρησης να επιβαρυνθεί με πρόστιμο εξαιτίας ενός τέτοιου συμβάντος.