Ανάλυση του malware «Stuxnet» από οργανισμό της ΕΕ: Παραδειγματική αλλαγή στις απειλές και την προστασία υποδομών πληροφοριών ζωτικής σημασίας.

Ο οργανισμός της Ευρωπαϊκής Ένωσης για την «ασφάλεια κυβερνοχώρου» ENISA, Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών, παρουσίασε τα αρχικά σχόλια και μια σύντομη, υψηλού επιπέδου ανάλυση των πρόσφατων επιθέσεων του «Stuxnet», σχετικά με τη σημασία τους και τις τεχνολογικές επιπλοκές για την Ευρώπη. Ο Οργανισμός θεωρεί ότι το «Stuxnet» συνιστά αλλαγή παραδείγματος και προειδοποιεί ότι είναι πιθανόν να συμβούν παρόμοιες επιθέσεις. Προτείνεται ότι η Ευρώπη πρέπει να αναθεωρήσει τα μέτρα προστασίας της για την προστασία υποδομών πληροφοριών ζωτικής σημασίας (CIIP).

Ο οργανισμός ENISA έχει παράγει μια υψηλού επιπέδου ανάλυση των επιπτώσεων του malware «Stuxnet». Ο σκοπός της μελέτης είναι να παρέχει στους υπεύθυνους λήψης αποφάσεων της Ευρωπαϊκής Ένωσης οδηγίες ώστε να μπορέσουν να κατανοήσουν το malware, τις ενδεχόμενες επιπτώσεις του, την αντιμετώπισή του, αλλά και για να κατανοήσουν την σημασία των νέου αυτού τύπου επιθέσεων για την Ευρώπη γενικότερα.

Ο εκτελεστικός διευθυντής του ENISA, Δρ.Udo Helmbrecht σχολιάζει:

«Το «Stuxnet» συνιστά πραγματικά αλλαγή παραδείγματος, καθώς αποτελεί μια καινούργια βαθμίδα και διάσταση όσον αφορά τα malware. Όχι μόνο από την άποψη της πολυπλοκότητας και της προηγμένης δομής του, καθώς π.χ. εκμεταλλεύεται συνδυαστικά τέσσερα διαφορετικά ευάλωτα σημεία των Windows, αλλά και με το να χρησιμοποιεί δύο κλεμμένα πιστοποιητικά και από εκεί να επιτίθεται στα περίπλοκα συστήματα SCADA της Siemens. Οι αρχιτέκτονες των επιθέσεων έχουν επενδύσει πολύ χρόνο και σημαντικά ποσά προκειμένου να δημιουργήσουν ένα τόσο πολύπλοκο εργαλείο επίθεσης. Το γεγονός ότι οι δράστες ενεργοποίησαν ένα τέτοιο εργαλείο επίθεσης, μπορεί να θεωρηθεί ως το «πρώτο χτύπημα», δηλαδή ως μία από τις πρώτες οργανωμένες, καλά προετοιμασμένες επιθέσεις ενάντια σε μείζονες βιομηχανικούς πόρους. Κάτι τέτοιο θα έχει τρομακτικό αντίκτυπο στον τρόπο προστασίας των εθνικών υποδομών πληροφοριών ζωτικής σημασίας (ΠΥΖΣ) στο μέλλον. Μετά το «Stuxnet»,η υφιστάμενη επικρατούσα φιλοσοφία για τις υποδομές πληροφοριών ζωτικής σημασίας θα πρέπει να αναθεωρηθεί. Θα πρέπει να δομηθεί με τέτοιο τρόπο ώστε να αντέχει στις νέες προηγμένες μεθόδους επίθεσης. Τώρα που το «Stuxnet» και οι υλοποιημένοι στόχοι του έχουν δημοσιοποιηθεί, είναι πιθανόν να αντιμετωπίσουμε περισσότερες επιθέσεις τέτοιου τύπου. Όλοι οι παράγοντες ασφαλείας θα πρέπει συνεπώς να συνεργάζονται πιο στενά και να αναπτύσσουν καλύτερες και πιο συντονισμένες στρατηγικές» καταλήγει ο Δρ.Helmbrecht.

Για μια **πιο αναλυτική τεχνική ανάλυση στο διαδίκτυο και για τις συστάσεις του Οργανισμού**, μεταβείτε εδώ.

Πώς ο οργανισμός ENISA υποστηρίζει τα Κράτη Μέλη ώστε να προετοιμαστούν ενάντια στις επιθέσεις στις κρίσιμες πληροφοριακές υποδομές;

Οι επιθέσεις μεγάλης κλίμακας ενάντια στις υποδομές πληροφοριών ζωτικής σημασίας απαιτούν συντονισμένες αντιδράσεις που θα εμπλέκουν όλους τους σημαντικούς παράγοντες τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Κανένα κράτος μέλος, προμηθευτής υλικού και λογισμικού, ομάδα αντιμετώπισης περιστατικών ασφάλειας (Cert- Computer Emergency and Response Team) ή φορέας επιβολής του νόμου δεν μπορεί μόνος του να αντιμετωπίσει προηγμένες επιθέσεις όπως αυτές του «Stuxnet».

Ο οργανισμός ENISA, ως φορέας εμπειρογνωμοσύνης στην ασφάλεια δικτύων και πληροφοριών (NIS), υποστηρίζει το σχέδιο δράσης της Ευρωπαϊκής Επιτροπής για την προστασία υποδομών πληροφοριών ζωτικής σημασίας (ΠΥΖΣ). Αυτό περιλαμβάνει στενή συνεργασία με τα κράτη μέλη, τους δημόσιους και τους ιδιωτικούς φορείς ώστε να διασφαλίσει την ασφάλεια των υποδομών πληροφοριών ζωτικής σημασίας της Ευρώπης.

Η ευελιξία του οργανισμού ENISA και το πρόγραμμα προστασίας υποδομών πληροφοριών ζωτικής σημασίας (CIPP) βοηθά τα κράτη μέλη και τον ιδιωτικό τομέα να αναπτύσσουν ορθές πρακτικές σε σειρά τομέων που συνδέονται με την προστασία υποδομών πληροφοριών ζωτικής σημασίας. Αυτό εμπεριέχει την καταπολέμηση δικτύων προγραμμάτων ρομπότ (botnet), βελτίωση της ασφάλειας των διασυνδεόμενων δικτύων και την αναφορά σημαντικών περιστατικών ασφάλειας. Το 2011 ο οργανισμός ENISA θα υποστηρίξει την ανάπτυξη ορθών πρακτικών στο πλαίσιο της ασφάλειας των συστημάτων SCADA και θα αναλύσει την εξάρτηση κρίσιμων τομέων με τις τεχνολογίες πληροφοριών και επικοινωνιών.

Επιπρόσθετα ο οργανισμός ENISA, σε συνεργασία με όλα τα κράτη μέλη της ΕΕ και 3 χώρες ΕΖΕΣ, συντονίζει την πρώτη πανευρωπαϊκή άσκηση ασφάλειας κυβερνοχώρου CIPP «CYBER EUROPE 2010».Αυτή η άσκηση θα ελέγξει τα σχέδια των κρατών μελών, τις πολιτικές και τις διαδικασίες για την αντιμετώπιση ενδεχομένων κρίσεων CIIP ή περιστατικά όπως αυτό του «Stuxnet».

Ο οργανισμός ENISA ενεργοποιείται επίσης στην ενίσχυση εθνικών/κυβερνητικών «ψηφιακών πυροσβεστικών», όπως οι Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας (CERT), παρέχοντας υποστήριξη στα κράτη μέλη για την εγκατάσταση, εκπαίδευση και εξάσκηση των ικανοτήτων αντιμετώπισης περιστατικών. Μαζί καθορίζουμε ένα επίπεδο βασικών ικανοτήτων που όλες οι ομάδες θα πρέπει να διαθέτουν. Επίσης εργαζόμαστε για τη βελτίωση των ικανοτήτων όπως π.χ. η διασυνοριακή συνεργασία, η Έγκαιρη Ειδοποίηση και η συνεργασία με τις αρχές επιβολής του νόμου.

Ο οργανισμός ENISA υποστηρίζει ενεργά τη συντονισμένη αντιμετώπιση επιθέσεων μεγάλης κλίμακας και θα αναλάβει πρόθυμα (εάν κληθεί) το ρόλο του συντονιστή και του υποστηρικτή στη λήψη των κατάλληλων μέτρων καταστολής.

Περαιτέρω πληροφορίες:

Πολλοί οργανισμοί NIS στα κράτη μέλη της ΕΕ κοινοποίησαν πληροφορίες για το «Stuxnet» στην αντίστοιχη γλώσσα τους. Ανατρέξτε στις αναφορές χωρών του ENISA για μια ανασκόπηση των δραστηριοτήτων ασφάλειας σε κάθε κράτος μέλος.

Για παράδειγμα, σε αυτούς τους δικτυακούς τόπους μπορείτε να βρείτε πληροφορίες για το ίδιο το malware, την αναγνώριση και την αντιμετώπισή του, κοινοποιημένες από (τους εξωτερικούς φορείς) Siemens και Symantec.

- Εργαλεία Siemens και διαδικασίες απομάκρυνσης
- Ανάλυση σε εξέλιξη του «Stuxnet» από τη Symantec
- Λευκή Βίβλος Stuxnet (PDF)
- Μπλογκ Ανταπόκρισης στο Stuxnet

Για συνεντεύξεις: Ulf Bergstrom, Εκπρόσωπος τύπου, ENISA, press@enisa.europa.eu,

Κινητό: + 30-6948-460-143

Για περισσότερες πληροφορίες επικοινωνήστε: Marco Thorbruegge, Sen.Exp. η με τον

Ulf Bergstrom, Υπεύθυνος Τύπου ENISA

Μετάφραση. Το αγγλικό πρωτότυπο είναι η μόνη έγκυρη εκδοχή.