ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΣΩΤΕΡΙΚΩΝ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΜΗΜΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Αθήνα, 24.1.2023
Αριθμ. Πρωτ: 5436

Πληροφορίες: Δρ. Κων/νος Ιωάννου
Ταχ. Δ/νση: Ευαγγελιστρίας 2
Ταχ. Κωδ.: 10183
Τηλέφωνο: 213 136 1022
Email: cybersecurity@ypes.gr

Προς

Διευθύνσεις και Τμήματα Πληροφορικής
Αποκεντρωμένων Διοικήσεων της Χώρας
Περιφερειών της Χώρας
και Δήμων της Χώρας

ΘΕΜΑ: Ενημέρωση για κυβερνοεπιθέσεις μέσω Phishing mails στο πλαίσιο του πολέμου στην Ουκρανία

Σας γνωρίζουμε ότι συνεχίζονται οι κακόβουλες επιθέσεις (phishing campaigns) εναντίον οργανισμών της Ουκρανίας, ευρωπαϊκών οργανισμών και υποδομών χωρών συμμάχων της Ουκρανίας (Λιθουανία, Πολωνία το 2023), με σκοπό την μόλυνση των υπολογιστών και την κυβερνοκατασκοπεία. Εκτιμάται ως πιθανό να επεκταθούν οι κακόβουλες ενέργειες και εναντίον του Ελληνικού κυβερνοχώρου. Συστήνουμε επαγρύπνηση και προετοιμασία ανίχνευσης και απόκρισης όπως παρακάτω.

Οι επιθέσεις πραγματοποιούνται μέσω της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν κακόβουλο λογισμικό σε συνημμένα συμπιεσμένα (.rar / .zip) αρχεία είτε συνδέσμους (hyperlinks) σε αυτά.

Οι συγκεκριμένες επιθέσεις έχουν αποδοθεί σε Ρώσους δρώντες (Gamaredon, Trident Ursa) με έντονη δραστηριότητα σε ουκρανικές υποδομές από την έναρξη του Ρωσοουκρανικού πολέμου.

Για τους παραπάνω λόγους συνιστάται αυξημένη επαγρύπνηση στη χρήση του ηλεκτρονικού ταχυδρομείου.

Προτείνεται να ληφθούν τα παρακάτω μέτρα:

- Έλεγχος της περιμέτρου της υποδομής και των τερματικών συσκευών για ενδείκτες παραβίασης και μπλοκάρισμά τους στα λογισμικά ελέγχου της περιμέτρου που χρησιμοποιείτε.

  Οι ενδείκτες παραβίασης (IoCs) περιλαμβάνονται στον παρακάτω σύνδεσμο:

  hxxps://github[.]com/pan-θnit42/iocs/blob/master/Gamaredon/Gamaredon_IoCs_DEC2022.txt

  Επιπλέον ενδείκτες παραβίασης είναι οι κάτωθι (IoCs):

  - ✓ κακόβουλη IP: 89.185.84[.]43
  - ✓ κακόβουλο URL: hxxp://194.180.174[.]158/18.01/quicker.rtf
  - ✓ κακόβουλο URL: hxxp://194.180.174[.]158/18.01/released.rtf

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

- Εφαρμόστε, αν είναι δυνατόν, πρόσθετο έλεγχο σε όλη την κίνηση του δικτύου σας που επικοινωνεί με το AS 197695 (Reg[.]ru).

Περισσότερες πληροφορίες είναι διαθέσιμες στον παρακάτω σύνδεσμο:

- hxxps://unit42.paloaltonetworks[.]com/trident-ursa/

Είμαστε στη διάθεσή σας για οποιαδήποτε διευκρίνηση ή αρωγή.

Ο Διευθυντής

Άγγελος Κουλός

Εσωτερική διανομή:

1. Γραφείο Υπουργού Εσωτερικών
2. Γραφείο Αναπληρωτή Υπουργού Εσωτερικών
3. Γραφείο Γενικού Γραμματέα Εσωτερικών και Οργάνωσης
4. Γραφείο Γενικού Διευθυντή Εσωτερικών και Ηλεκτρονικής Διακυβέρνησης