DTS MALWARE ATTACK SIMULATION

Η υπηρεσία Malware Attack Simulation είναι μια προσφορά που απευθύνεται αποκλειστικά σε νέους πελάτες της DTS. Βάσει του μοντέλου Assume Breach αξιολογούμε κατά πόσο είναι δυνατή η εγκατάσταση κακόβουλου λογισμικού στο δίκτυο της επιχείρησης και η απόκτηση απομακρυσμένου ελέγχου σε αυτό μέσω τεχνικών Command-and-Control - C2.

ΔΥΟ ΣΕΝΑΡΙΑ ΠΡΟΣ ΕΠΙΛΟΓΗ:

- Απόπειρα κυβερνοεπίθεσης μέσω Ransomware
- Απόπειρα κυβερνοεπίθεσης με στόχο τη βιομηχανική κατασκοπεία

Στόχος της αξιολόγησης είναι ο εντοπισμός κενών ασφαλείας, ικανά να επιτρέψουν σε κάποιον να παραβιάσει το πληροφοριακό σας σύστημα, να υποκλέψει δεδομένα ή ακόμη και να διαταράξει κρίσιμες επιχειρηματικές διαδικασίες.

Ερωτήματα που καλούμαστε να απαντήσουμε σε κάθε σενάριο:

- Σενάριο Ransomware: Πόσο ανθεκτική είναι η επιχείρηση απέναντι σε επιθέσεις που στοχεύουν στην κρυπτογράφηση δεδομένων και στον εκβιασμό; Μπορεί ένας επιτιθέμενος να εγκαταστήσει κακόβουλο λογισμικό, να το εξαπλώσει σε όλη την επιχείρηση και να διατηρήσει τον έλεγχο εξ' αποστάσεως;
- Σενάριο Βιομηχανικής Κατασκοπείας: Πόσο ευάλωτη είναι η επιχείρηση σε θέματα κλοπής ευαίσθητων δεδομένων μέσω στοχευμένων επιθέσεων; Μπορεί ένας επιτιθέμενος να εγκαταστήσει κακόβουλο λογισμικό και να μεταφέρει τελικά προς τα έξω κρίσιμες πληροφορίες μέσω ενός C2-καναλιού (Command-and-Control).

ΤΙ ΠΕΡΙΛΑΜΒΑΝΕΙ (ΜΕΘΟΔΟΛΟΓΙΑ)

1. Ανάλυση Ευπαθειών: Συλλέγουμε πληροφορίες για τις υποδομές μιας επιχείρησης και προχωράμε στην ανάλυσή τους, με στόχο τον εντοπισμό πιθανών κενών ασφαλείας έναντι επιθέσεων malware.
2. Προσομοίωση ρεαλιστικών επιθέσεων malware: Οι ειδικοί κυβερνοασφάλειας της DTS διεξάγουν πολλαπλά σενάρια, με στόχο την προσπάθεια εγκατάστασης malware και δημιουργίας ενός μη ανιχνεύσιμου C2-καναλού για τον απομακρυσμένο έλεγχο των κρίσιμων υποδομών. Χρησιμοποιούνται σύνηθες μέθοδοι του MITRE ATT&CK Framework, όπως π.χ.: Execution, Persistence, Defense Evasion και Command-and-Control, θεωρώντας ότι η παραβίαση υποδομών έχει ήδη επιτευχθεί.
3. Αποτίμηση: Εξετάζουμε και αξιολογούμε τη δυνατότητα του εισβολέα να εισχωρήσει και να εξαπλωθεί στο εσωτερικό δίκτυο της επιχείρησης:
   - Lateral Movement: Με πλάγιο τρόπο, αξιοποιώντας την επικοινωνία με άλλες δικτυακές συσκευές
   - Privilege Escalation: Με απόκτηση δικαιωμάτων διαχείρισης
   - Credential Access: Με κλοπή διαπιστευτηρίων
   - Collection: Με συλλογή δεδομένων από το παραβιασμένο σύστημα
   - Command and Control: Με τη δημιουργία καναλιού επικοινωνίας για απομακρυσμένο έλεγχο
   - Exfiltration: Μεταφορά δεδομένων εκτός συστήματος

ΑΝΑΛΥΤΙΚΑ Η ΔΙΑΔΙΚΑΣΙΑ

- Προετοιμασία: Παρέχονται συσκευές και στοιχεία πρόσβασης, καθώς και εγγραφή στην πλατφόρμα αναφορών DTS
- Εναρκτήρια Συνάντηση: Καθορισμός τεχνικών λεπτομερειών & στόχων της αξιολόγησης
- Εκτέλεση: Διεξαγωγή της άσκησης αξιολόγησης εξαπολύοντας εικονικές επιθέσεις, ανάλυση και τεκμηρίωση των ευρημάτων
- Τελική Συνάντηση: Παρουσίαση αποτελεσμάτων και προτάσεις μέτρων αντιμετώπισης
- Προαιρετικά: Δυνατότητα περαιτέρω ανάλυσης & επανελέγχων μέσω της πλατφόρμας DTS

ΤΑ ΟΦΕΛΗ ΣΑΣ

- Μέσω των στοχευμένων προσομοιώσεων malware-attacks εντοπίζονται ευπάθειες και κενά ασφαλείας, απ' όπου θα μπορούσε να εγκατασταθεί κακόβουλο λογισμικό
- Προσαρμογή της αξιολόγησης στις επιχειρηματικές ανάγκες και τους στόχους της στρατηγικής ασφάλειας της επιχείρησης
- Εκτίμηση της αποτελεσματικότητας των υπαρχόντων μέτρων ασφάλειας
- Προτάσεις για τις αναγκαίες άμεσες ενέργειες που απαιτούνται για την αντιμετώπιση κρίσιμων ευπαθειών, καθώς και για την μακροπρόθεσμη βελτίωση της στρατηγικής ασφαλείας

DTS Cloud Security MonEPE - Athens
+30 211 1040-710

dts.de/el
info@dts-cloudsecurity.gr

DTS Malware Attack Simulation 15042025