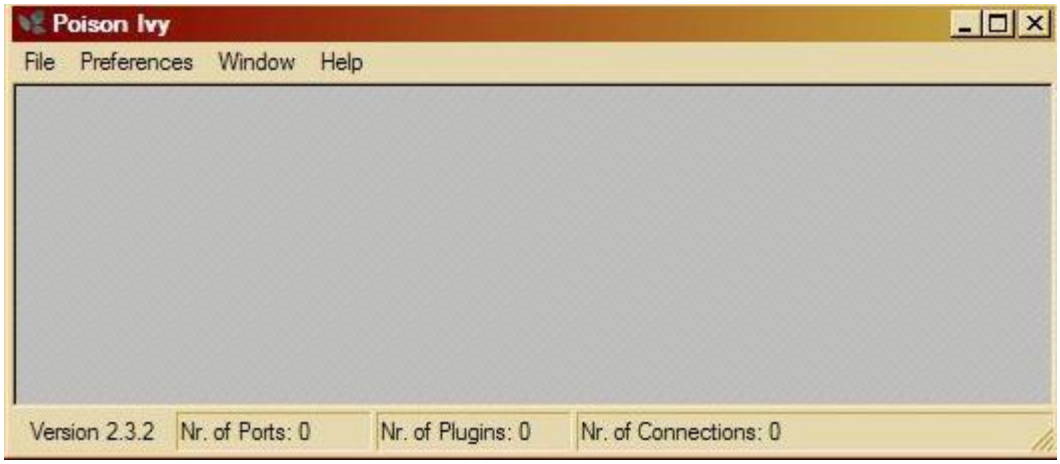
Threat Actor – Ron Aldo



Καθώς εργαζόσασταν σήμερα στην εταιρεία σας ως υπεύθυνος Κυβερνοασφάλειας, δεχτήκατε μια επίθεση από έναν επιτιθέμενο με ψευδώνυμο Ron Aldo. Μετά από αυτό το συμβάν, θέλετε να ετοιμάσετε ένα report που θα αναλύει τη συγκεκριμένη επίθεση με το πρότυπο STIX2 ώστε να μπορέσετε να το μοιραστείτε και να βοηθήσετε άλλους οργανισμούς να προστατευθούν από αυτόν τον επιτιθέμενο και τις δράσεις του. Οι πληροφορίες που συλλέξατε για τον συγκεκριμένο threat actor είναι οι ακόλουθες:

- Το ψευδώνυμό του είναι Ron Aldo.
- Είναι γνωστό ότι χρησιμοποιεί phising επιθέσεις για να παραδώσει remote access malware στους στόχους του.
- Θεωρείται κατάσκοπος και εγκληματίας.
- Άλλο ψευδώνυμο με το οποίο έχει συσχετιστεί ο επιτιθέμενος είναι το Uncatchable.
- Πρώτη φορά που παρατηρήθηκε ήταν 2015-05-07T14:22:14.760Z
- Οι στόχοι του είναι να καταφέρει να υποκλέψει εμπιστευτικά αρχεία.
- Σχετικά με την κατάρτισή του θεωρείται expert.
- Επίσης αναφέρεται πως επιτίθεται μόνος.

- Ο τρόπος που επιτίθεται είναι μέσω phising.
- Πιο συγκεκριμένα χρησιμοποιεί spear phising σαν μηχανισμό παράδοσης του malware του.
- Σχετικά με το kill chain της mand-attack-lifecycle-model , το όνομα του σταδίου kill chain του μοτίβου επίθεσης, θεωρείται το initial-compromise.
- Σαν εξωτερικές αναφορές, το μοτίβο επίθεσής του που παρατηρείται είναι το CAPEC-98 (https://capec.mitre.org/data/definitions/98.html)

- Ο Ron Aldo στην επίθεση που επιχείρησε, χρησιμοποίησε το malware Posion Ivy Variant d1c9, το οποίο είναι τύπου remote-access-trojan.
- Σαν περιγραφή του malware αναφέρθηκε το παρακάτω κείμενο: When installed, it allows the virus to control the infected computer. It then opens a backdoor to allow the virus in. When in control, Poison Ivy can record or manipulate the computer

or activate the webcam and speaker to record audio and video.

- Το συγκεκριμένο malware δεν αντιπροσωπεύει κάποιο malware family.

- Σχετικά με το kill chain της mand-attack-lifecycle-model , το όνομα του σταδίου kill chain του malware, θεωρείται το initial-compromise.

- Αυτό το malware γράφτηκε σε γλώσσα προγραμματισμού Assembly (Implementation language vocabulary: x86-64)

- Ακόμα αναφέρεται πως αυτό το malware κλέβει authentication credentials.

- Επίσης σαν custom fields (allow_custom=True) δίνεται το sha256 hash για το συγκεκριμένο malware:

sha256= ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

---

- Ο Ron Aldo χρησιμοποιεί το Poison Ivy.
- Ο Ron Aldo χρησιμοποιεί το phising.

ΟΔΗΓΙΕΣ:

Διαβάστε καλά το stix2 specification που υπάρχει στην εκπαιδευτική δραστηριότητα αλλά και τους τρόπους δημιουργίας stix2 περιεχομένου. Ξεκινήστε αναγνωρίζοντας ποια είναι τα stix2 SDO και ποια τα πεδία τους που θα ορίσετε μέσα από τα δεδομένα. Για τα custom πεδία δώστε και το πεδίο allow_custom=True. Τα πεδία created,modified αν δεν τα ορίσετε παίρνουν αυτόματα τιμή το τωρινό timestamp, μπορείτε να το παραλείψετε είτε να το συμπληρώσετε. Προσοχή, στα δεδομένα, εκεί που δίνεται ακριβές timestamp (first_seen) θα βάλετε αυτό που ορίζεται. Οποιοδήποτε άλλο πεδίο είναι required πρέπει να το συμπληρώσετε για να δημιουργηθεί το αντικείμενο. Στα SRO πρέπει να συσχετίσετε τα αντικείμενα μεταξύ τους. Επειδή σε ένα relationship SRO πρέπει να δώσετε τα stix2 id των 2 αντικειμένων στα source_ref ,target_ref (relationship_type το ορίζετε με ένα string κανονικά), προτείνω να χρησιμοποιήσετε τη μέθοδο parse της βιβλιοθήκης stix2, που κάνει parsing το αντικείμενο και μπορείτε να πάρετε το id μετά. Στο τέλος, μέσω της βιβλιοθήκης stix2 θα βάλετε όλα τα αντικείμενα SDO και SRO σε ένα bundle και αποθήκευση του σε ένα αρχείο προς παράδοση. Τα προαναφερθέν είναι για την περίπτωση που χρησιμοποιήσετε τον τρόπο της python. Στη συνέχεια το bundle το ανεβάζετε στον stix visualizer ,βγάζετε screenshot και ανεβάζετε το αρχείο και την εικόνα στο classroom.

Καλή επιτυχία!!