Diamond Model

-Đế Tọa-

I.Over view

Mô Hình Kim Cương của Phân Tích Xâm Nhập được phát triển bởi các chuyên gia an ninh mạng - Sergio Caltagirone, Andrew Pendergast và Christopher Betz vào năm 2013.

Như mô tả bởi những người sáng tạo, Mô Hình Kim Cương được tạo thành từ bốn yếu tố cốt lõi: đối thủ, cơ sở hạ tầng, khả năng và nạn nhân, và xác định yếu tố nguyên tử cơ bản của bất kỳ hoạt động xâm nhập nào. Bạn có thể cũng đã chú ý đến hai yếu tố hoặc trục bổ sung của Mô Hình Kim Cương - Xã Hội, Chính Trị và Công Nghệ; chúng ta sẽ đi vào chi tiết hơn về chúng sau trong phòng này. Tại sao nó được gọi là "Mô Hình Kim Cương"? Bốn đặc điểm cốt lõi này được kết nối với nhau ở cạnh, đại diện cho mối quan hệ cơ bản của chúng và được sắp xếp theo hình dạng của một viên kim cương.

Mô Hình Kim Cương mang theo các khái niệm cơ bản của phân tích xâm nhập và hoạt động của đối thủ trong khi vẫn cho phép linh hoạt mở rộng và bao gồm ý tưởng và khái niệm mới. Mô hình cung cấp nhiều cơ hội để tích hợp thông tin tình báo theo thời gian thực để phòng ngự mạng, tự động hóa sự tương quan qua các sự kiện, phân loại sự kiện với sự tự tin vào các chiến dịch của đối thủ và dự báo hoạt động của đối thủ trong quá trình lên kế hoạch và chiến lược giảm thiểu.

Tại sao bạn nên học về Mô Hình Kim Cương?

Mô Hình Kim Cương có thể giúp bạn xác định các yếu tố của một sự xâm nhập. Ở cuối phòng này, bạn sẽ tạo ra một Mô Hình Kim Cương cho các sự kiện như sự vi phạm, xâm nhập, tấn công hoặc sự cố. Bạn cũng sẽ có khả năng phân tích Mối Đe Dọa Tổng Hợp (APT).

Mô Hình Kim Cương cũng có thể giúp giải thích cho những người không chuyên ngành về những gì đã xảy ra trong một sự kiện hoặc bất kỳ thông tin quý báu nào về kẻ đe dọa độc hại.

II. Theory

1.Adversary

Một **Advensary** còn được biết đến là một kẻ tấn công, đối thủ, nhà hành vi đe dọa mạng hoặc hacker. Kẻ đối thủ là người đứng đằng sau cuộc tấn công mạng. Các cuộc tấn công mạng có thể là một hành động chỉ đạo hoặc một vi phạm.

Theo những người sáng tạo của Mô Hình Kim Cương, kẻ đối thủ là một cá nhân hoặc tổ chức chịu trách nhiệm sử dụng một khả năng chống lại nạn nhân để đạt được mục đích của họ. Kiến thức về kẻ đối thủ thường có thể là bí ẩn, và đặc điểm cốt lõi này có thể trống rỗng đối với hầu hết các sự kiện - ít nhất là vào thời điểm phát hiện.

Quan trọng là phải biết sự phân biệt giữa người vận hành của kẻ đối thủ và khách hàng của kẻ đối thủ vì điều này sẽ giúp bạn hiểu rõ về mục đích, xác định, sự thích ứng và sự kiên trì bằng cách giúp xây dựng mối quan hệ giữa một cặp đối thủ và nạn nhân.

Việc xác định kẻ đối thủ trong giai đoạn đầu của một cuộc tấn công mạng là khó khăn. Việc sử dụng dữ liệu được thu thập từ một sự cố hoặc vi phạm, các chữ ký và thông tin khác có liên quan có thể giúp bạn xác định người có thể là kẻ đối thủ.

Người Vận Hành của **Advensary** là "hacker" hoặc cá nhân(s) thực hiện hoạt động xâm nhập.

Khách Hàng của **Advensary** là thực thể hưởng lợi từ hoạt động được thực hiện trong sự xâm nhập. Nó có thể là cùng một người đứng đằng sau người vận hành của kẻ đối thủ, hoặc nó có thể là một người hoặc nhóm riêng lẻ.

Ví dụ, một khách hàng của kẻ đối thủ có thể kiểm soát đồng thời nhiều người vận hành khác nhau. Mỗi người vận hành có thể có khả năng và cơ sở hạ tầng riêng.

Answer the questions below

What is the term for a person/group that has the intention to perform malicious actions against cyber resources?

adversary operator

What is the term of the person or a group that will receive the benefits from the cyberattacks?

Adversary customer

2.Victim

Nạn nhân – là một mục tiêu của kẻ đối thủ. Một nạn nhân có thể là một tổ chức, cá nhân, địa chỉ email mục tiêu, địa chỉ IP, tên miền, v.v. Quan trọng là phải hiểu sự khác biệt giữa nhân cách của nạn nhân và tài sản của nạn nhân vì chúng phục vụ các chức năng phân tích khác nhau.

Một nạn nhân có thể là một cơ hội cho những kẻ tấn công để đặt chân vào tổ chức mà họ đang cố gắng tấn công. Luôn có một nạn nhân trong mọi cuộc tấn công mạng. Ví dụ, một email spear-phishing (một email được tạo ra một cách tỉ mỉ nhắm vào một người cụ thể) được gửi đến công ty, và một ai đó (nạn nhân) đã nhấp vào liên kết. Trong trường hợp này, nạn nhân là mục tiêu được chọn của kẻ đối thủ.

Nhân cách của Nạn Nhân là những người và tổ chức được nhắm đến và tài sản của họ đang bị tấn công và lợi dụng. Điều này có thể là tên tổ chức, tên người, ngành công nghiệp, vai trò công việc, sở thích, v.v.

Tài sản của Nạn Nhân là bề mặt tấn công và bao gồm bộ hệ thống, mạng, địa chỉ email, máy chủ, địa chỉ IP, tài khoản mạng xã hội, v.v., mà kẻ đối thủ sẽ hướng đến bằng khả năng của họ.

Answer the questions below

What is the term that applies to the Diamond Model for organizations or people that are being targeted?

Victim Personae

3.Capability

Khả năng – còn được biết đến là kỹ năng, công cụ và kỹ thuật được kẻ đối thủ sử dụng trong một sự kiện. Khả năng làm nổi bật các chiến thuật, kỹ thuật và thủ tục của kẻ đối thủ (TTPs).

Khả năng có thể bao gồm tất cả các kỹ thuật được sử dụng để tấn công nạn nhân, từ những phương pháp ít phức tạp, chẳng hạn như đoán mật khẩu thủ công, đến những kỹ thuật phức tạp nhất, như phát triển malware hoặc công cụ độc hại.

Sức chứa của Khả năng là tất cả các lỗ hổng và phơi bày mà khả năng cụ thể có thể sử dụng.

Bộ Vũ Khí của Kẻ Đối Thủ là một bộ khả năng thuộc sở hữu của một kẻ đối thủ. Sức chứa kết hợp của các khả năng của một kẻ đối thủ tạo nên Bộ Vũ Khí của họ.

Một kẻ đối thủ phải có các khả năng cần thiết. Các khả năng có thể là kỹ năng phát triển malware và email lừa đảo hoặc ít nhất là truy cập vào các khả năng, chẳng hạn như việc mua lại malware hoặc ransomware dưới dạng dịch vụ.

Answer the questions below

Provide the term for the set of tools or capabilities that belong to an adversary.

adversary arsenal

4.Infrastructure

Cơ sở hạ tầng – còn được biết đến là phần mềm hoặc phần cứng. Cơ sở hạ tầng là sự kết nối vật lý hoặc logic mà kẻ đối thủ sử dụng để triển khai một khả năng hoặc duy trì kiểm soát các khả năng. Ví dụ, một trung tâm điều khiển và kiểm soát (C2) và kết quả từ nạn nhân (lấy dữ liệu).

Cơ sở hạ tầng cũng có thể là địa chỉ IP, tên miền, địa chỉ email, hoặc thậm chí là một thiết bị USB độc hại được tìm thấy trên đường và được cắm vào một máy trạm.

Cơ sở hạ tầng Loại 1 là cơ sở hạ tầng do kẻ đối thủ kiểm soát hoặc sở hữu.

Cơ sở hạ tầng Loại 2 là cơ sở hạ tầng do một bên trung gian kiểm soát. Đôi khi bên trung gian có thể hay không có thể biết đến nó. Đây là cơ sở hạ tầng mà một nạn nhân sẽ nhìn thấy như là của kẻ đối thủ. Cơ sở hạ tầng Loại 2 có mục đích làm mờ nguồn gốc và đặc điểm của hoạt động. Cơ sở hạ tầng Loại 2 bao gồm máy chủ lưu trữ malware, tên miền độc hại, tài khoản email bị nhiễm bệnh, v.v.

Nhà Cung Cấp Dịch Vụ là tổ chức cung cấp các dịch vụ được coi là quan trọng cho sự tồn tại của Cơ sở hạ tầng Loại 1 và Loại 2 của kẻ đối thủ, ví dụ như Nhà Cung Cấp Dịch Vụ Internet, đăng ký tên miền và nhà cung cấp email trực tuyến.

Answer the questions below

To which type of infrastructure do malicious domains and compromised email accounts belong?

Type 2 infrastructure

What type of infrastructure is most likely owned by an adversary?

Type 1 infrastructure

5.Event Meta Features

Có thể thêm vào Diamond Model sáu meta-đặc điểm khác nhau. Các meta-đặc điểm không bắt buộc, nhưng chúng có thể thêm vào mô hình Diamond một số thông tin hoặc thông tin tình báo quan trọng.

Timestamp - là ngày và giờ của sự kiện. Mỗi sự kiện có thể được ghi lại với một ngày và giờ xảy ra, chẳng hạn như 2021-09-12 02:10:12.136. Timestamp có thể bao gồm cả thời gian bắt đầu và kết thúc của sự kiện. Timestamps là quan trọng để giúp xác định các mô hình và nhóm các hoạt động độc hại. Ví dụ, nếu xâm nhập hoặc vi phạm xảy ra vào lúc 3 giờ sáng ở Hoa Kỳ, có thể có khả năng rằng cuộc tấn công được thực hiện từ một quốc gia cụ thể có múi giờ khác nhau và giờ làm việc chuẩn.
Phase - đây là các giai đoạn của một cuộc xâm nhập, tấn công hoặc vi phạm. Theo những người tạo ra Diamond Model và Axiom 4, "Mọi hoạt động độc hại chứa đựng hai hoặc nhiều giai đoạn cần phải được thực hiện thành công liên tiếp để đạt được kết quả mong muốn." Các hoạt động độc hại không xảy ra như là các sự kiện đơn lẻ, mà thay vào đó là một chuỗi sự kiện. Một ví dụ tuyệt vời có thể là Chuỗi Hạm Đánh Máy Máy Tính được phát triển bởi Lockheed Martin. Bạn có thể tìm hiểu thêm về Chuỗi Hạm Đánh Máy Máy Tính bằng cách truy cập phòng Cyber Kill Chain trên TryHackMe.
Result - Trong khi kết quả và điều kiện sau cùng của các hoạt động của đối thủ không luôn được biết đến hoặc có giá trị tin cậy cao khi biết đến, chúng hữu ích để ghi lại. Quan trọng là ghi lại kết quả và điều kiện sau cùng của các hoạt động của đối thủ, nhưng đôi khi chúng có thể không luôn được biết đến. Kết quả sự kiện có thể được gán nhãn là "thành công," "thất bại," hoặc "không xác định." Kết quả sự

kiện cũng có thể liên quan đến triad CIA (bảo mật, tính toàn vẹn và tính sẵn có), chẳng hạn như "Bảo mật bị xâm phạm," "Tính toàn vẹn bị xâm phạm," và "Tính sẵn có bị xâm phạm." Một cách tiếp cận khác cũng có thể là ghi lại tất cả các điều kiện sau cùng của sự kiện, ví dụ như thông tin được thu thập trong giai đoạn tìm hiểu hoặc lấy mật khẩu/thông tin nhạy cảm thành công.
Direction - Đặc điểm meta này giúp mô tả các sự kiện dựa trên máy chủ và mạng và đại diện cho hướng của cuộc tấn công xâm nhập. Mô hình Diamond của Phân Tích Xâm Nhập định nghĩa bảy giá trị tiềm năng cho đặc điểm meta này: Nạn nhân-đến-Cơ sở hạ tầng, Cơ sở hạ tầng-đến-Nạn nhân, Cơ sở hạ tầng-đến-Cơ sở hạ tầng, Đối thủ-đến-Cơ sở hạ tầng, Cơ sở hạ tầng-đến-Đối thủ, Hai chiều hoặc Không xác định.
Methodology - Đặc điểm meta này sẽ cho phép một nhà phân tích mô tả phân loại chung của cuộc xâm nhập, chẳng hạn như lừa đảo, tấn công từ chối dịch vụ (DDoS), vi phạm, quét cổng, vv.
Resources - Theo Diamond Model, mỗi sự kiện xâm nhập cần một hoặc nhiều nguồn lực bên ngoài để đảm bảo sự hài lòng và thành công. Ví dụ về các nguồn lực có thể bao gồm: phần mềm (ví dụ: hệ điều hành, phần mềm ảo hóa hoặc khung Metasploit), kiến thức (ví dụ: cách sử dụng Metasploit để thực hiện cuộc tấn công và chạy khai thác), thông tin (ví dụ: tên người dùng/mật khẩu để giả mạo), phần cứng (ví dụ: máy chủ, máy trạm, router), tiền (ví dụ: tiền để mua tên miền), cơ sở vật chất (ví dụ: điện hoặc nơi ẩn náu), quyền truy cập (ví dụ: một đường mạng từ máy chủ nguồn đến nạn nhân và ngược lại, quyền truy cập mạng từ nhà cung cấp dịch vụ Internet (ISP)).

Answer the questions below

What meta-feature does the axiom "Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result" belong to?

phase

You can label the event results as "success", "failure", and "unknown". What meta-feature is this related to?

result

To what meta-feature is this phrase applicable "Every intrusion event requires one or more external resources to be satisfied prior to success"?

resource

6. Social-Political Component

Thành phần xã hội-chính trị mô tả những nhu cầu và ý định của đối thủ, ví dụ như lợi nhuận tài chính, được chấp nhận trong cộng đồng hacker, hoạt động hacktivism hoặc gián điệp.

Tình huống có thể là nạn nhân cung cấp một "sản phẩm", chẳng hạn như tài nguyên máy tính và băng thông như một con zombie trong một botnet cho mục đích đào tiền điện tử (tạo ra tiền điện tử mới bằng cách giải các phương trình mật mã thông qua việc sử dụng máy tính), trong khi đối thủ tiêu thụ sản phẩm của họ hoặc đạt được lợi nhuận tài chính

7.Technology Component

Công nghệ - đặc điểm hay thành phần công nghệ meta-feature làm nổi bật mối quan hệ giữa các đặc điểm cốt lõi: khả năng và cơ sở hạ tầng. Khả năng và cơ sở hạ tầng mô tả cách đối thủ hoạt động và truyền thông. Một kịch bản có thể là cuộc tấn công "vũ trụ nước" (watering-hole), là một phương pháp mà đối thủ t compromised (bị xâm phạm) các trang web hợp pháp mà họ tin rằng những nạn nhân mục tiêu của họ sẽ truy cập.

8.Practice Analysis

THM{DIAMOND_MODEL_ATTACK_CHAIN}