Fragebogen zur Erstellung von Knotenwahrscheinlichkeitstabellen für Bayes’sche Netze

Name:
Datum:

Aufgabe 1: Noisy-OR-Modell

Hintergrund

Das Noisy-OR-Modell ist eine Methode zur Modellierung von Wahrscheinlichkeiten, bei der angenommen wird, dass jede Ursache unabhängig das Zielereignis auslösen kann – aber nicht mit absoluter Sicherheit.
Mehrere Ursachen erhöhen die Wahrscheinlichkeit, dass das Zielereignis eintritt.
Jede Ursache wird durch einen Gewichtungsfaktor beschrieben, der angibt, wie stark sie das Zielereignis beeinflusst (von 0 = kein Einfluss bis 1 = maximaler Einfluss).
Zusätzlich wird oft ein Leakage-Faktor berücksichtigt. Dieser beschreibt die Wahrscheinlichkeit, dass das Zielereignis auch ohne die bekannten Ursachen eintreten kann – etwa durch unbekannte oder nicht modellierte Faktoren.

Modell

Du bewertest im Folgenden verschiedene Anzeichen darauf, wie stark sie auf die Technik **"T1048 – Exfiltration Over Alternative Protocol"** hindeuten.
Bitte nutze eine Skala von **0** (geringste Relevanz) bis **1** (höchste Relevanz).

Fragen

1. Alternative Exfiltration via Cloud Services

Merkmal:
Ungewöhnliche Datei-Uploads über Cloud-Dienste wie Google Drive, OneDrive oder E-Mail-Versand von großen Dateien.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

2. Suspicious Cloud Storage Access

Merkmal:
Ungewöhnliche oder verdächtige Zugriffe auf Cloud-Speicher, etwa durch viele Dateifreigaben oder Downloads in kurzer Zeit, oder unerwartete Quellen.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

3. Alternative Protocol Exfiltration via Command Execution

Merkmal:
Ausführung von Befehlen wie `scp`, `ftp`, `curl`, `wget`, `tar`, `7zip`, die für alternative Datenübertragungen genutzt werden können.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

4. File Access Before Exfiltration

Merkmal:
Zugriff auf sensible Dateien (.pdf, .docx, .jpg usw.) in isolierten Pfaden oder ungewöhnlichen Kontexten vor einer möglichen Exfiltration.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

5. Outbound Connections Over Non-Standard Ports

Merkmal:
Verbindungen zu externen Zielen über ungewöhnliche Ports (z. B. FTP: 21, SMTP: 25/587, SMB: 445), mit großen Datenmengen und auffälliger Häufigkeit.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

6. Anomalies in Protocol Traffic

Merkmal:
Verdächtige Netzwerkverkehrsmuster oder Anomalien in der Protokollstruktur, z. B. Pakete, die nicht zu etablierten Verbindungen passen oder ungewöhnliche Syntax verwenden.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

7. Unusual Network Flows

Merkmal:
Unerwartete Netzwerkaktivitäten von Prozessen, die normalerweise keine Verbindungen initiieren, oder neue, bisher unbekannte Datenflüsse.

Frage:
Welchen Gewichtungsfaktor ordnest du diesem Merkmal hinsichtlich seiner Aussagekraft für das Vorliegen von Datenexfiltration über alternative Protokolle (T1048) zu?
Antwort: _____

---

8. Leakage-Faktor

Frage:
Wie hoch schätzt du die Wahrscheinlichkeit, dass eine Exfiltration über alternative Protokolle stattfindet, **selbst wenn keiner der oben genannten Faktoren beobachtet wird**?
(Antworte mit einem Wert zwischen **0** und **1**.)
Antwort: _____

---

9. Sicherheit der Einschätzungen

Frage:
Wie sicher bist du dir bei deinen Einschätzungen?
(Skala **1** = sehr unsicher bis **10** = absolut sicher)
Antwort: _____

---

10. Verständnis

Frage:
Hast du die Aufgabenstellung verstanden?
(Antworte bitte mit **Ja** oder **Nein**.)
Antwort: _____

T1048

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels.

Exfiltration Over Alternative Protocol can be done using various common operating system utilities such as Net/SMB or FTP.[1] On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.[2]

Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or Cloud API.

DS0015

Monitor cloud-based file hosting services, such as Google Drive and Microsoft OneDrive, for unusual instances of file downloads – for example, many downloads by a single user in a short period of time. In environments with high-maturity, it may be possible to leverage User-Behavioral Analytics (UBA) platforms to detect and alert on user-based anomalies. Additionally, data loss prevention policies can be defined to detect and alert on exfiltration events on particularly sensitive data.

DS0010

Monitor for unusual queries to the cloud provider's storage service. Activity originating from unexpected sources may indicate improper permissions are set and are allowing access to data. Additionally, detecting failed attempts by a user for a certain object, followed by escalation of privileges by the same user, and access to the same object may be an indication of suspicious activity.

DS0017

Monitor executed commands and arguments that may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.

DS0022

Monitor for suspicious files (i.e. .pdf, .docx, .jpg, etc.) viewed in isolation that may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.

DS0029.001

Monitor for outbound connections using non-standard ports for FTP, SMTP, or SMB, new processes generating large amounts of outbound traffic, or traffic flows that do not align with normal business usage patterns.

DS0029.002

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

DS0029.003

Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.