

Name : Amr Khaled Elgendi
Group : AMIT - Cyber Security Online 87
Task : MITRE ATT&CK Framework

Scenario

You are hired as a Blue Team member for a company. You are assigned to perform threat intelligence for the company. See how you can operationalize the MITRE ATT&CK framework to solve these scenario-based problems

Q1 : Your company heavily relies on cloud services like Azure AD, and Office 365 publicly. What technique should you focus on mitigating, to prevent an attacker performing Discovery activities if they have obtained valid credentials? (Hint: Not using an API to interact with the cloud environment!)

T1538

which focuses on preventing an adversary which may use a cloud service GUI with stolen credentials to gain useful information from an operational environment.

Q2 : You were analyzing a log and found uncommon data flow on port 4050. What APT group might this be?

G0099

A screenshot of a log entry. The log entry shows a single row of data. The first column is a timestamp and task ID, followed by the source IP, destination IP, port, and protocol. The log entry is as follows:

port 4050	APT-C-36, Blind Eagle, Group G0099	...ened.[1] Enterprise T1036.004 Masquerading: Masquerade Task or Service APT-C-36 has disguised its scheduled tasks as those used by Google.[1] Enterprise T1571 Non-Standard Port APT-C-36 has used port 4050 for C2 communications.[1] Enterprise T1027 Obfuscated Files or Information APT-C-36 has used ConfuserEx to obfuscate its variant of Imminent Monitor, compressed payload and RAT packages, and password...
-----------	------------------------------------	--

Q3 : The framework has a list of 9 techniques that falls under the tactic to try to get into your network. What is the tactic ID?

TA0008

try to get into your network (lateral movement)

Q4 : A software prohibits users from accessing their account by deleting, locking the user account, changing password etc. What such software has been documented by the framework?

S0372

A screenshot of a search interface. The search bar at the top contains the text "software lock". Below the search bar, there is a single search result card. The result card has a dark grey header with the text "S0372" and "Lock" repeated twice. The main content area of the card shows the following information:
Link: [Lockergoga, Software S0372](#)
Description: ... Norsk Hydro's production systems were impacted by a Lockergoga infection. This resulted in a loss of view which forced the company to switch to manual operations. [4] [5] Groups That Use This Software ID Name References G0037 FIN6 [6] References Harbison, M. (2019, March 26). Born This Way? Origins of Lockergoga. Retrieved April 16, 2019. CarbonBlack Threat Analysis Unit. (2019, March 22). TAU Threat Intelligence Notification – Lockergoga Ransomware. Retrieved April 16, 2019. Greenberg, A. (2019, March...
A red "X" button is located in the top right corner of the result card.

Q5 : Using ‘Pass the Hash’ technique to enter and control remote systems on a network is common. How would you detect it in your company?

Audit all logon and credential use events and review for discrepancies