**Operating Systems**

If a host has a series of logs with Event ID 4625 followed by one with Event ID 4624, what could this be indicative of?

**Failed login is 4625 and 4624 is an indication that an account has been successfully logged onto. Meaning this could potentially be a brute force attack where the attacker used multiple passwords until one worked.**

**Networking**

What can be used for application whitelisting on Linux based systems?

**applications to be used for whitelisting on Linux: INTEGRITY MEASUREMENT ARCHITECTURE OR RED HAT ENTERPRISE LINUX 8.**

**Security Principles**

Why is it important to remove or disable stale accounts in an environment?

They are able to cause fatal damages to an organization, especially when they are not disabled or when they remain without password expiry limits. Outside intruders trying to hack into an organization can use these accounts as their activities will go unnoticed. Also, employees who quit the organization can misuse their login credentials to access network resources.

**Cyber Threat Intelligence**

Using information from this recent CTI report, provide examples for each of the four points of the Diamond Model.

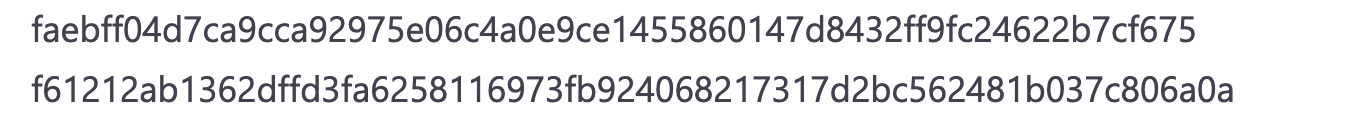
<https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/>

ADVESARY:

GADOLINIUM

CAPABILITIES:

Hashes associated with malicious documents:



Actor Owned email addresses:

Chris.sukkar@hotmail.com  
PhillipAdamsthird@hotmail.com  
sdfwfde234sdws@outlook.com  
jenny1235667@outlook.com  
fghfert32423dsa@outlook.com  
sroggeveen@outlook.com  
RobertFetter.fdmed@hotmail.com  
Heather.mayx@outlook.com

VICTIMS:

cloud services

maritime

health industries

Asia Pacific region

higher education and regional government organizations.

INFASTRUCTURE:

spear-phishing emails with malicious attachments

command & control

malicious code

PowerShell commands

Remote access