***A Sample Ransomware attack on an XYZ mining Company***

Sending a mail to any one of the employees such that,

Hello,

This mail is from a higher authority, to notify you that your employment with Emp\_Id MA 243013244 is being terminated. You have violated the following company policy :

[Rule 67.3 Article 2](file:///C:\Users\DELL\OneDrive\Documents\Rule%2067.3%20Article%202)

[Rule 69.4 Article 1](file:///C:\Users\DELL\OneDrive\Documents\Rule%2069.4)

You were issued written warnings on 18.08.2021, to take steps to correct your behaviour by 01.09.2021. Your failure to do so has given rise to termination in your service.

Sincerely,

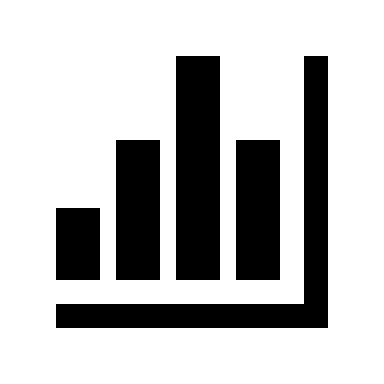
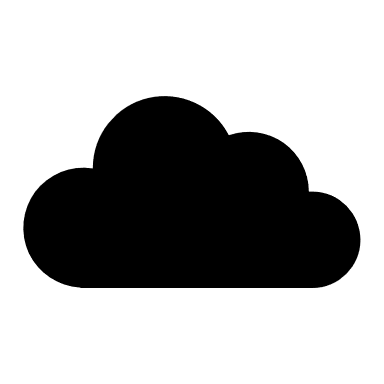
ABX XYZ

Authentication Head

XYZ Mining

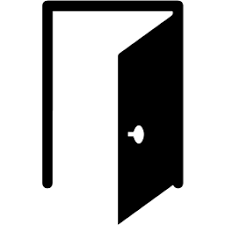
Out of Curiosity, the employee will click on any of the hyperlinks provided. On doing so, a malicious document downloads a backdoor, so that hackers can access a target system without having to go through the usual authentication steps. Then Visual Basic script gets downloaded, which runs some PowerShell code[ Ip address control ], which downloads some executable file, which later downloads the main malware

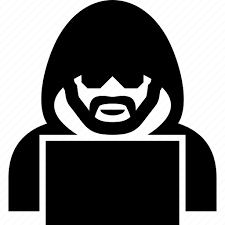
***A GENERAL RANSOMWARE ATTACK MIND-MAP***



Hacker gets access over the employees’ system

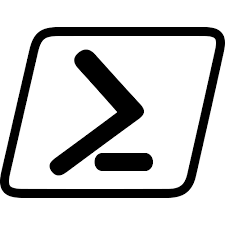
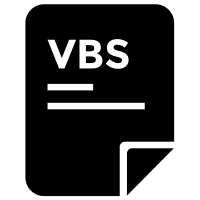
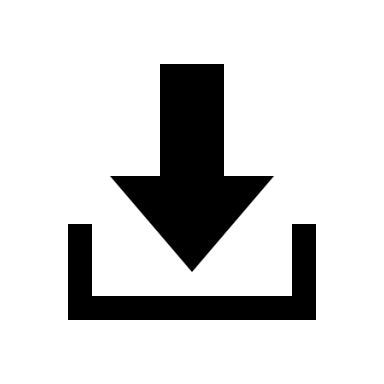
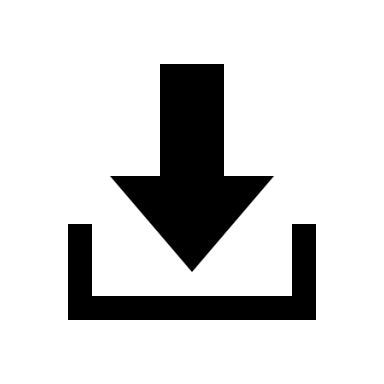
Back Door





IP related details

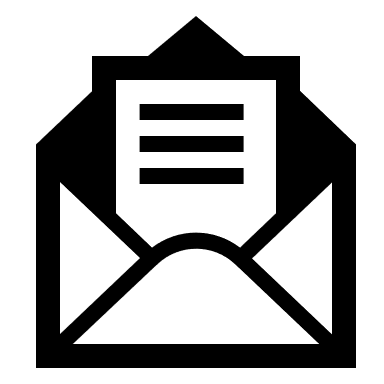
Hacker



EXE

User selects

hyperlink

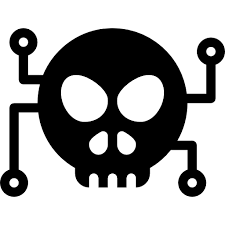
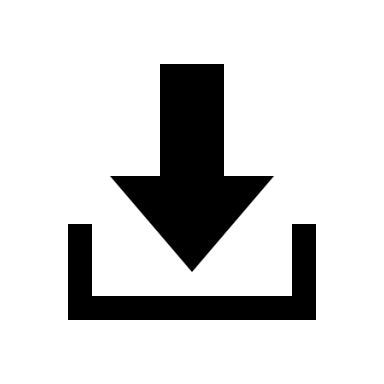


Downloads VB script

executable file is downloaded

PowerShell gets run

Employee receives mail



Main Malware is downloaded

Attackers carry out disturbance approaches like :

1. Setting up Connect Availability group liseners, to extend the time of data accessing without being detected.
2. Connect-back approach, to connect the tarfget network and their control server, so they can send the stolen data to their server in a safe manner

Though backdoor attacks are designed to be undiscoverable, we can reduce their effect by following strategies :

1. Using anti-malware
2. Setting up Firewalls to limit access to only legal users, those employees’ having authentication and keep a 24/7 team to monitor the network continuously and update the system on a regular basis.