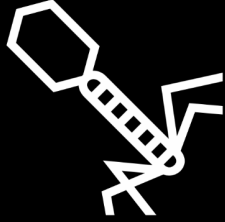


5 

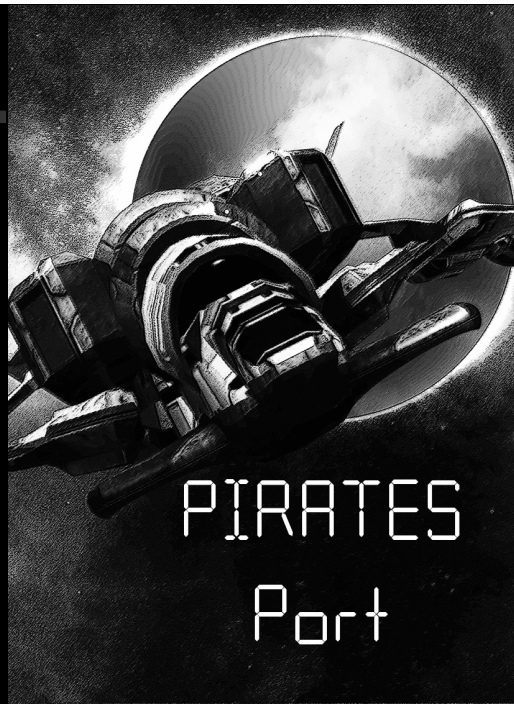
Persistent Malware



COST  8  DMG  2



Obfuscated code saved to the
Common Log File System



Take a card from the event
row for free

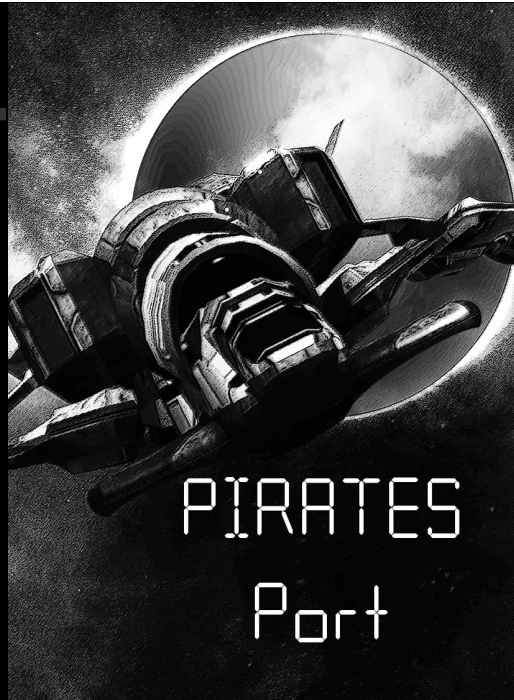
Signed Driver



COST  10  DMG  2



Signed Razer mouse driver
privilege escalation

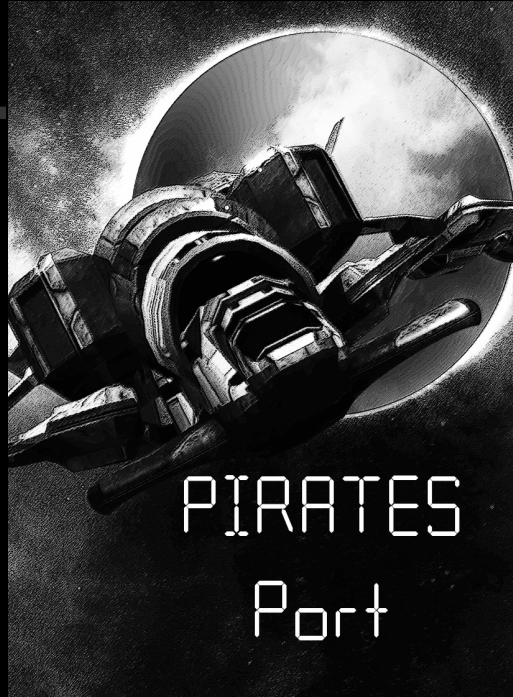


Draw a Card

Browser Plugin



Malicious Chrome extension
supply chain attack



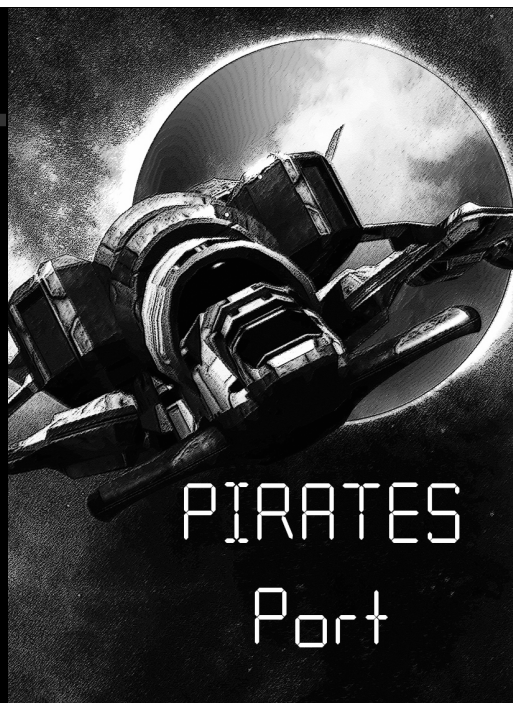
1 

Draw a Card

Malicious Driver



Malicious driver deployed for
keyboard input interception

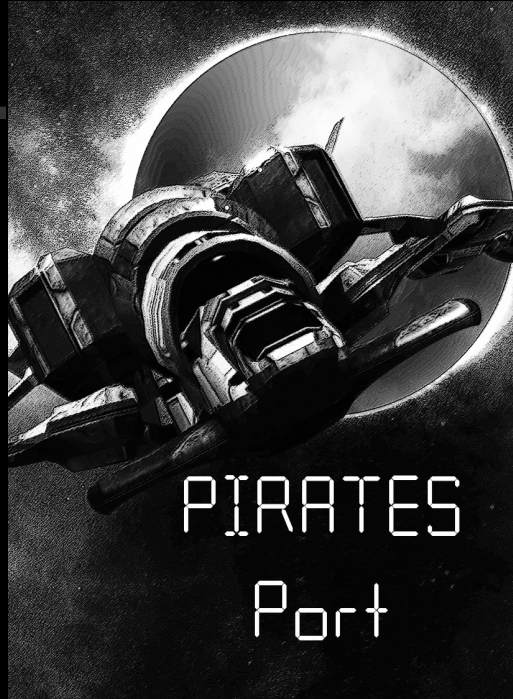


Copy a card in your hand

New Service



Persistence using Windows service disguised as EDR updater



PIRATES
Port

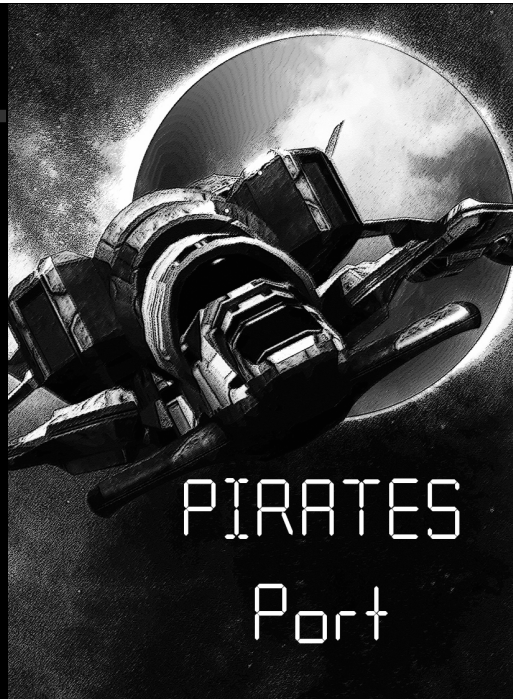
2 

Draw a Card

Cloud Bucket



Data exfiltration through public cloud storage bucket



PIRATES
Port

1 

Draw a Card

New User Added



COST 

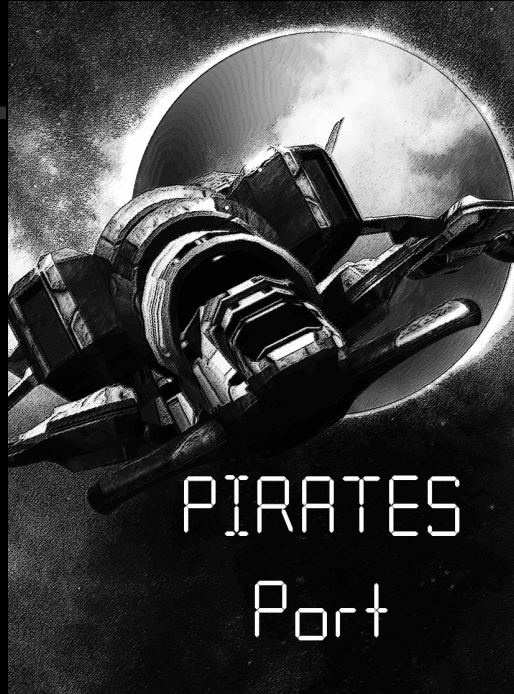
4



DMG



New user assetmgt created
with administrator access



6 

Draw a Card

Cloud Metadata



COST 

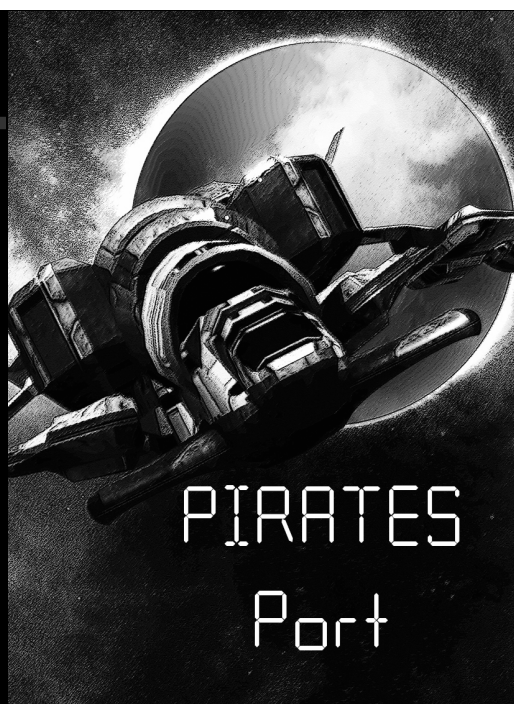
10



DMG



Cloud access through
Instance Metadata Service
exfiltration



5

Multi-Factor Auth.



COST

6

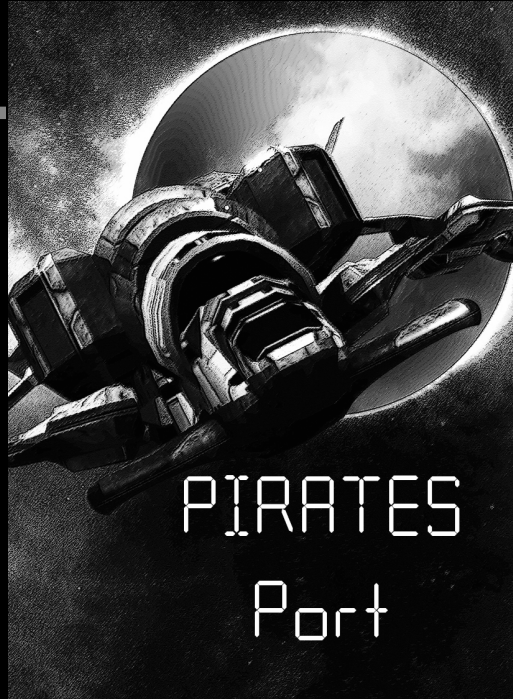


DMG

2



MFA use denies attacker
access to application access



PIRATES
Port

Use a card from your discard

Watering Hole



COST



8

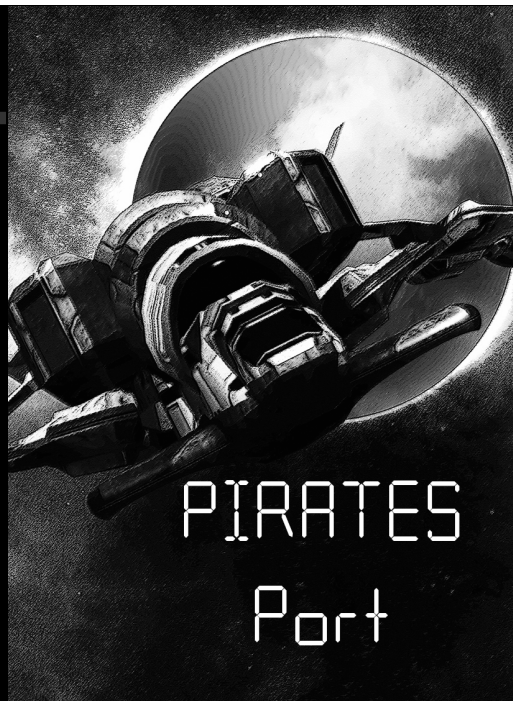


DMG

3



Redirected to malicious
website through Facebook
Messenger



PIRATES
Port

5



Cloud Account



COST



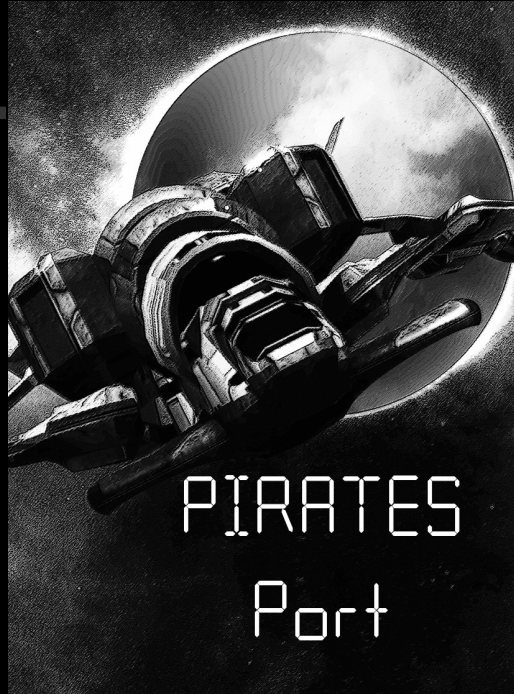
8



DMG



Endpoints compromised
through O365 Ruler payload
delivery



3



Credential Stuffing



COST



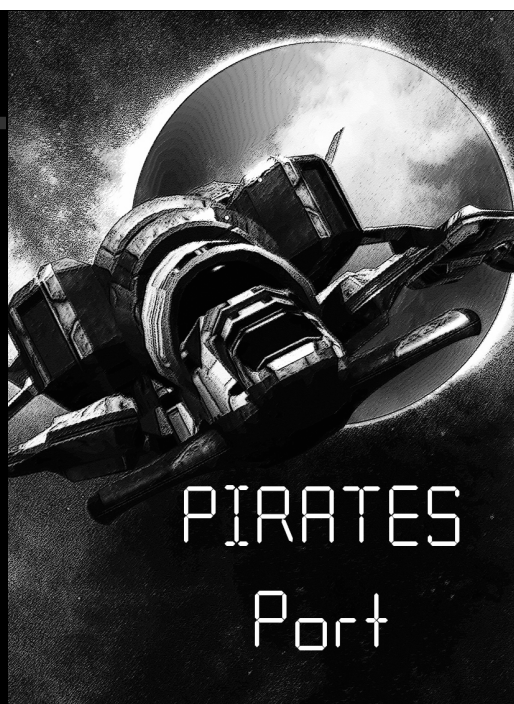
4



DMG

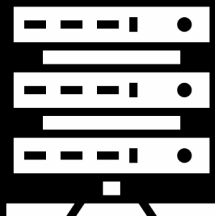


Citrix internal network access
through reused credentials



2

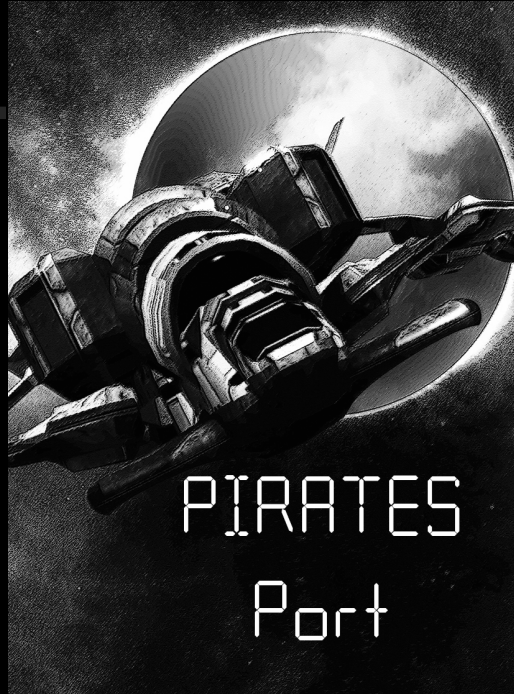
Web Shell



1



Persistent access to web server with isolated code



1

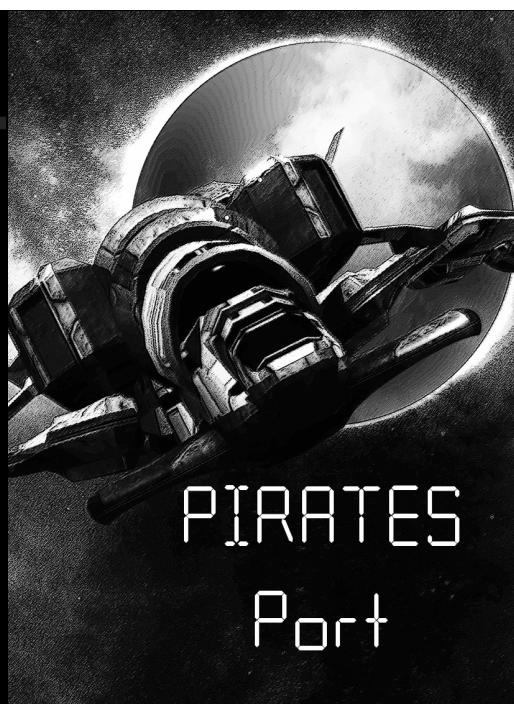
Malicious Kubelet



2



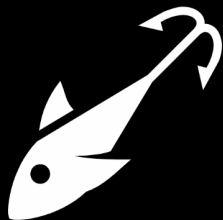
Kubernetes takeover with malicious kubelet deployment



3 

Draw a Card

Fake Installer

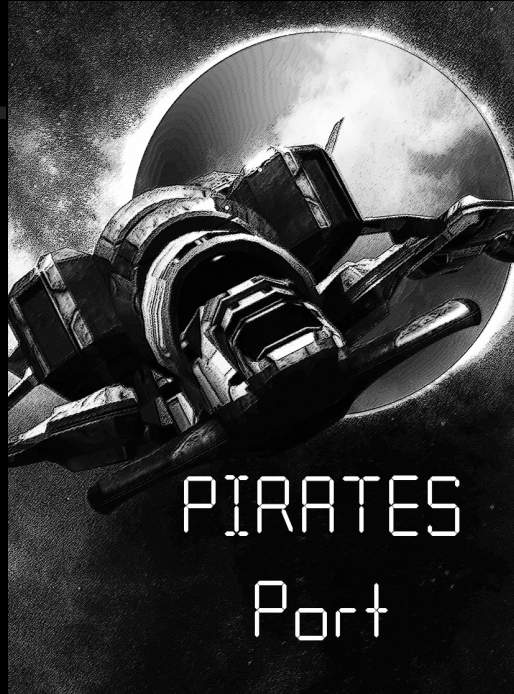


COST  4

DMG  4



Gain access through a fake installer



Draw a Card

O365 Macro

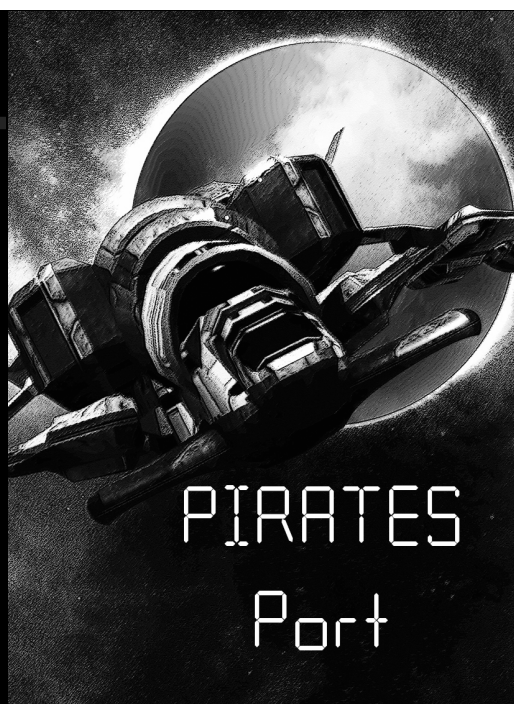


COST  1

DMG  6



Command execution through O365 Excel document macro



2 

Draw a Card

Sysmon Reporting

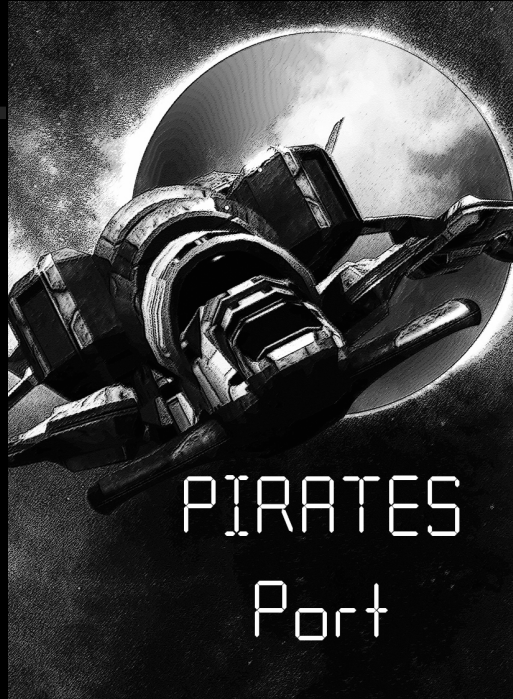


COST  4

DMG  3



Malicious PowerShell invocation detected



PIRATES Port

4 

Shadow Copy

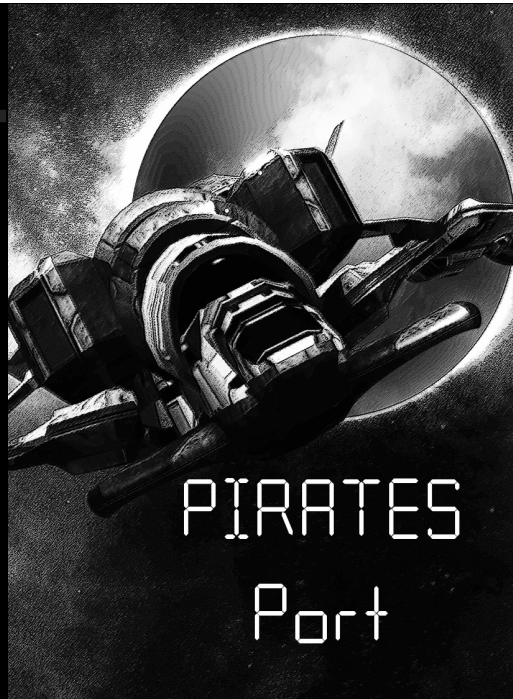


COST  5


DMG  3



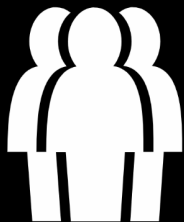
Access protected SAM database using Volume Shadow Copy



PIRATES Port

1  Draw a Card

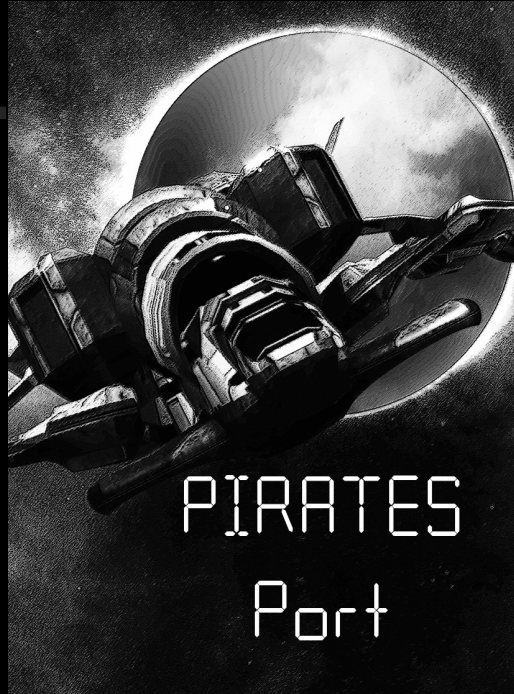
Password Audit




COST  4 DMG  3



DPAT reveals systemic password selection exposure



PIRATES
Port

1  Draw a Card

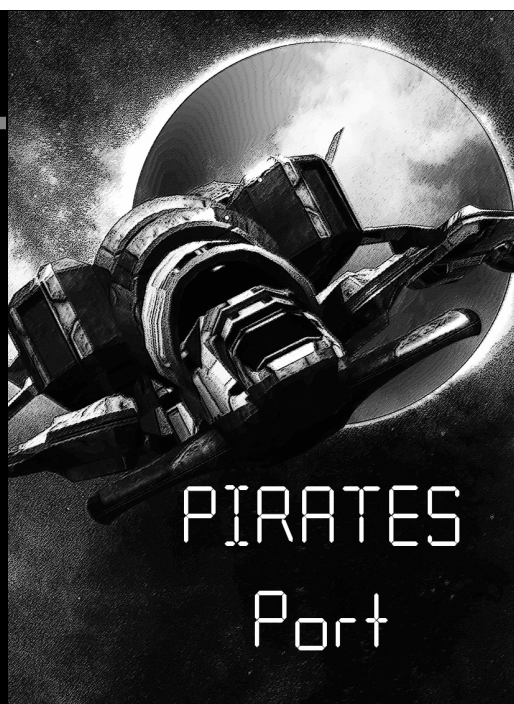
Sinkhole Domain



COST 2  DMG  5



Malicious activity identified through a sinkhole DNS response



PIRATES
Port

2 

Log Analysis



COST

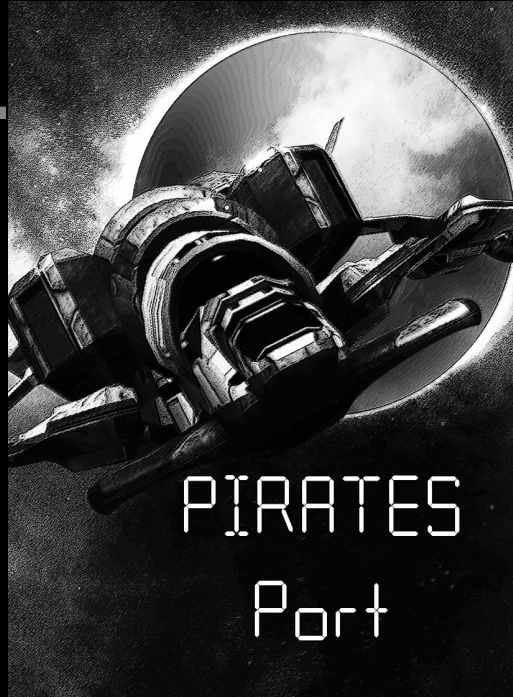
1



DMG



SIEM logging analysis
identifies APT activity



PIRATES
Port

2 

Draw a Card

Endpoint Detection



COST

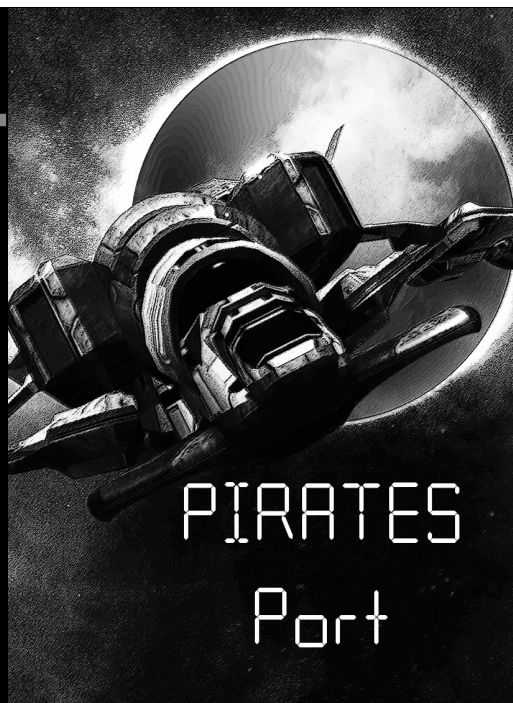
3



DMG



EDR identifies program
execution blocked by safe list



PIRATES
Port

4 

User Behavior



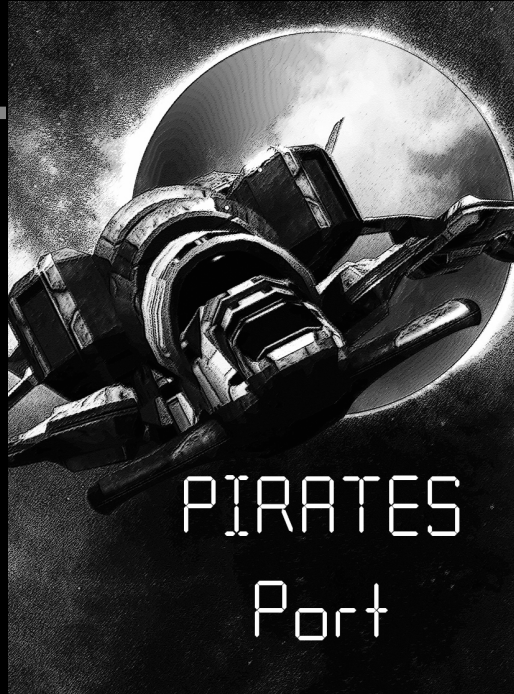
COST

5 

DMG 



UEBA suspends cmd.exe
process launched from
LSASS



6 

Draw a Card

MFA Bypass



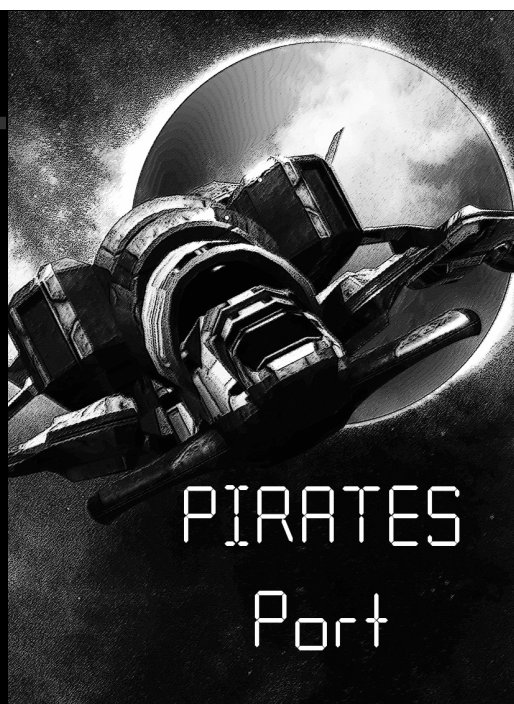
COST

 10 

DMG 



Office 365 MFA bypass using
named location access



5 

Zero Trust



COST

6

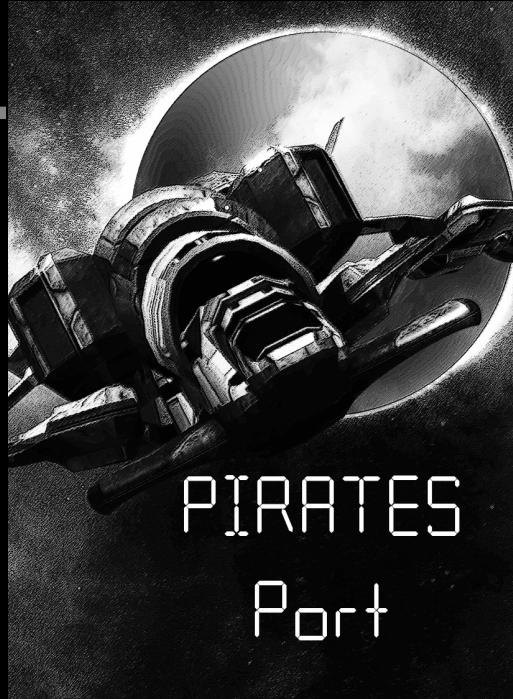


DMG

2



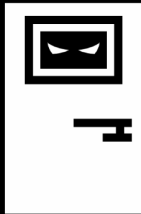
Assumed breach principle
mitigates scope of incident



2 

Draw a Card

Identity Mgmt



COST

4

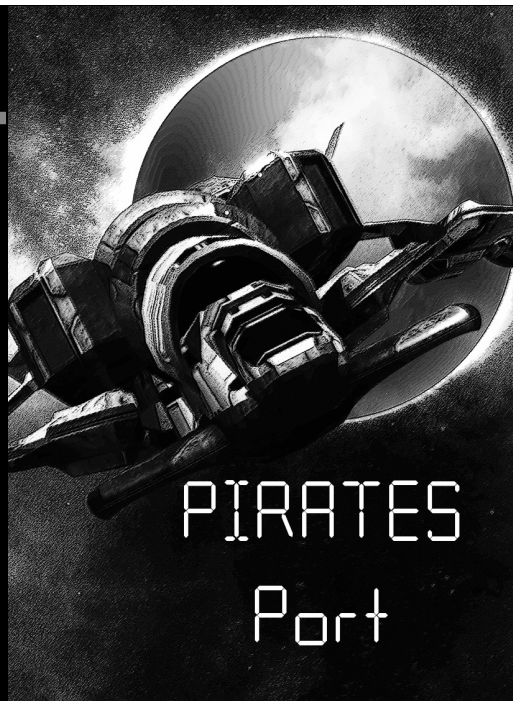


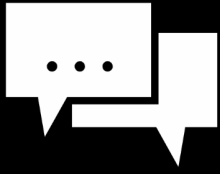
DMG

3

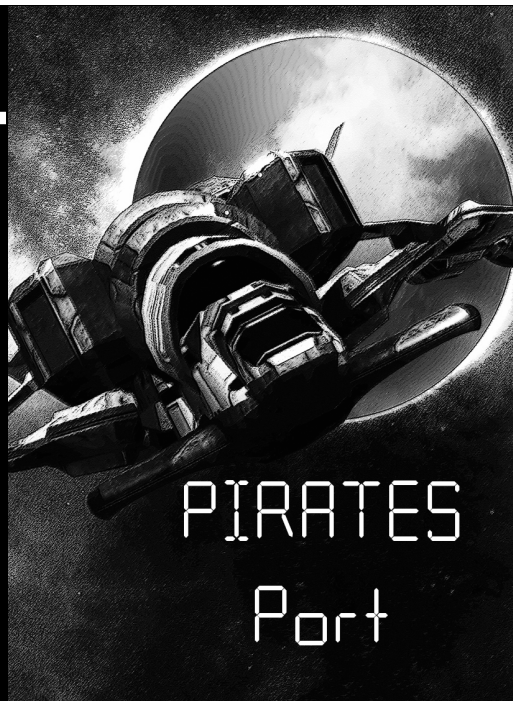
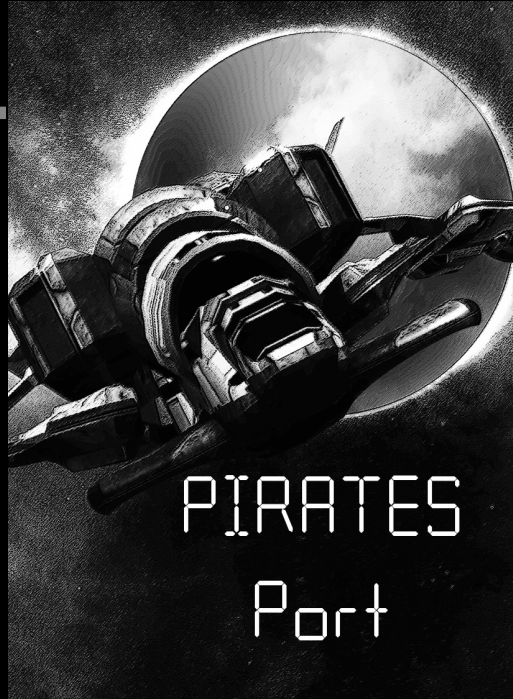


JIT/JEA policies stop
unauthorized use and
privilege escalation





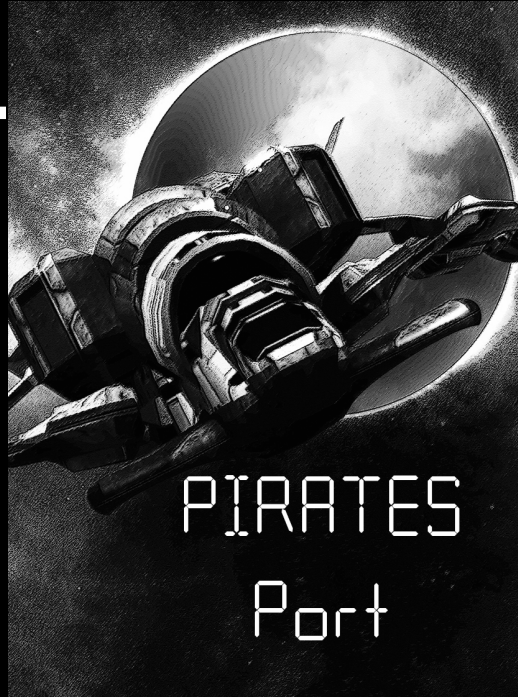
Identify attack activity with
SRUM-Dump



1 

P1

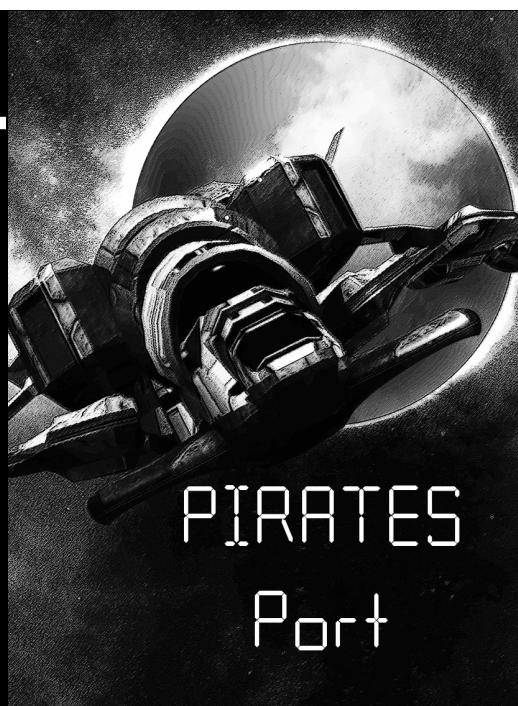
Skill



1 

P1

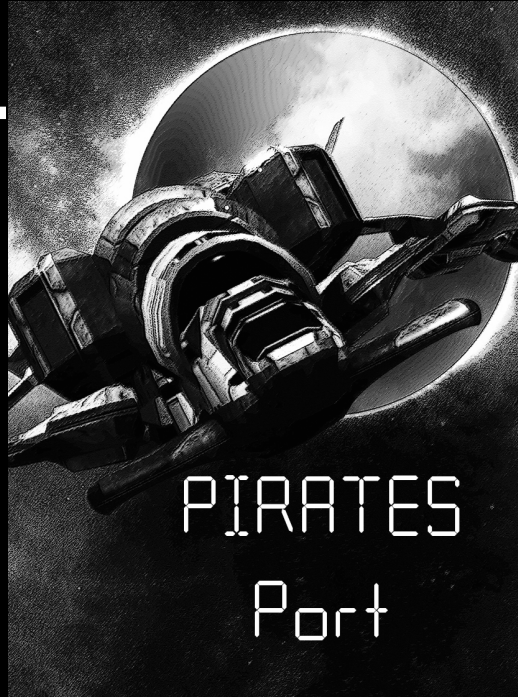
Skill



1 

P1

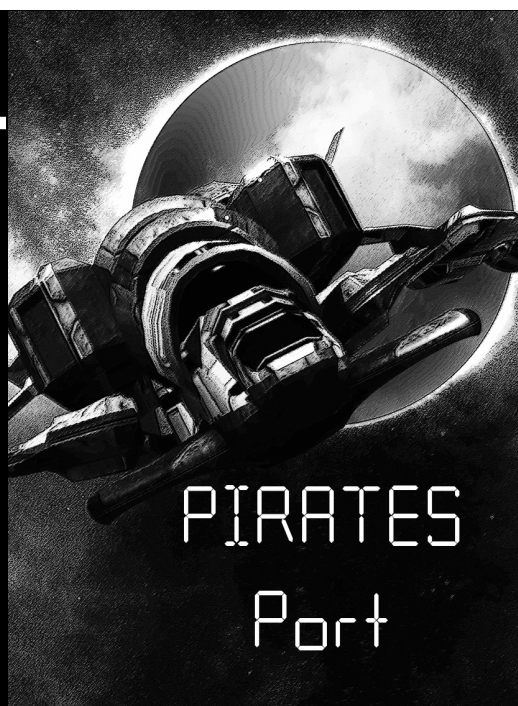
Skill

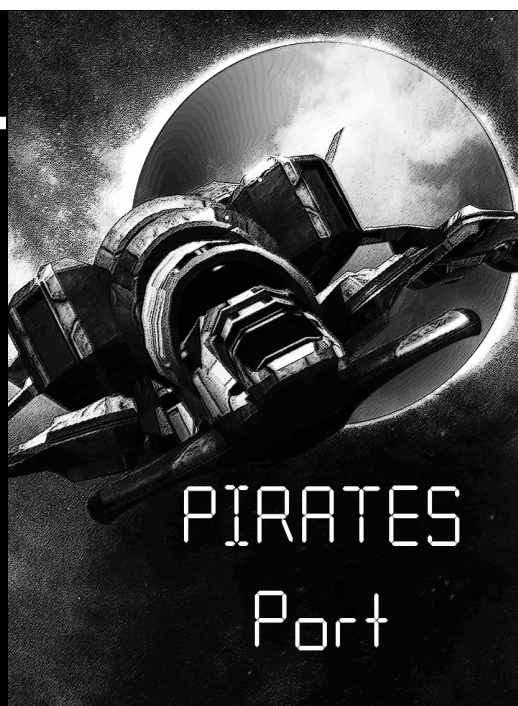
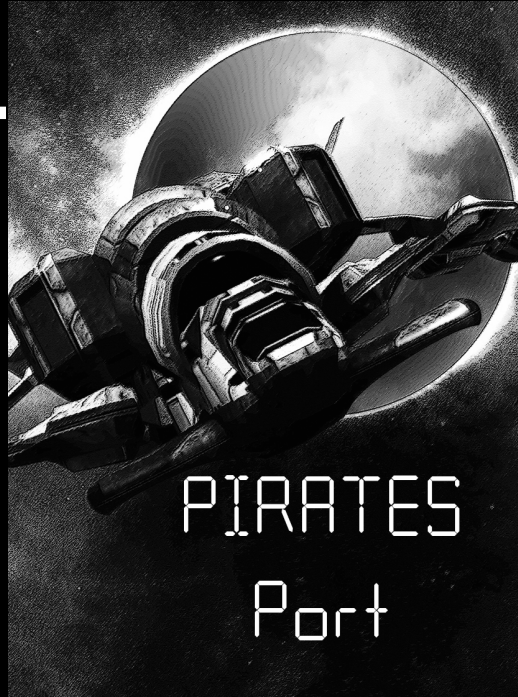


1 

P2

Skill

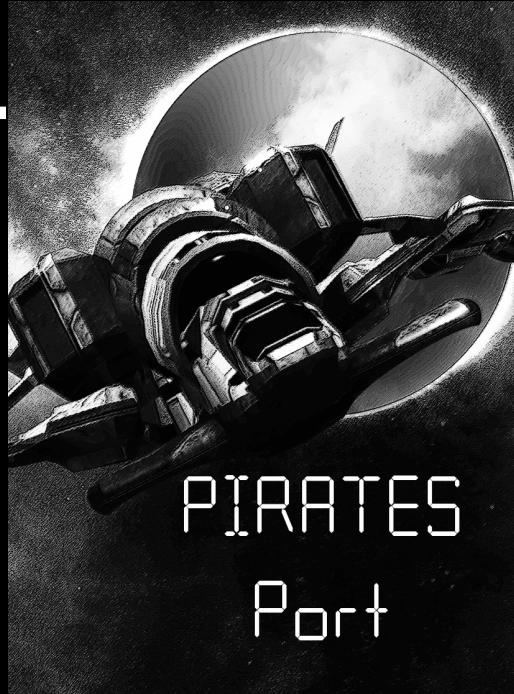




1 

P2

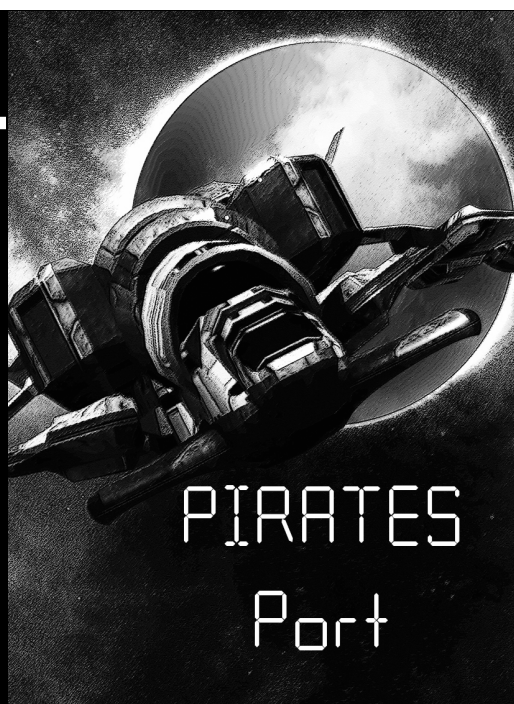
Skill

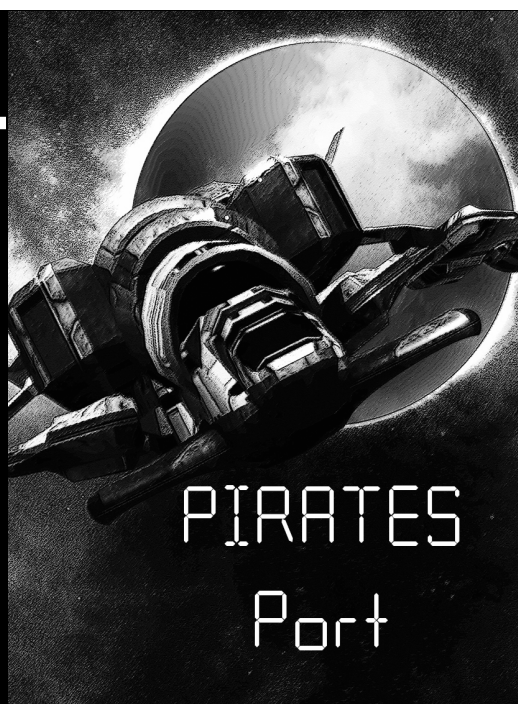
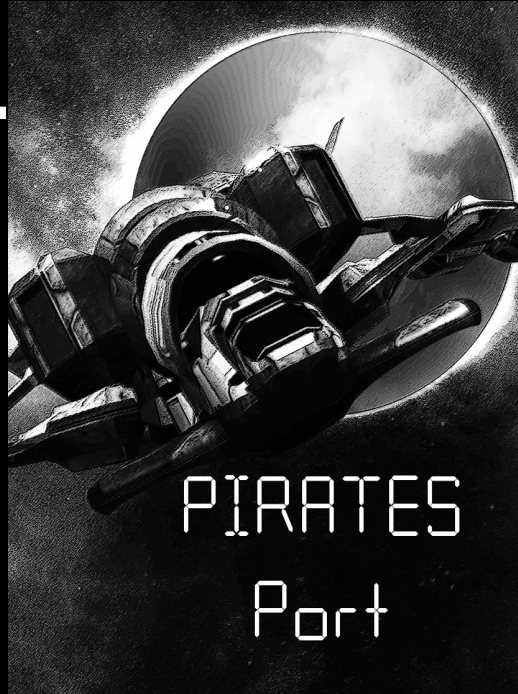


1 

P3

Skill

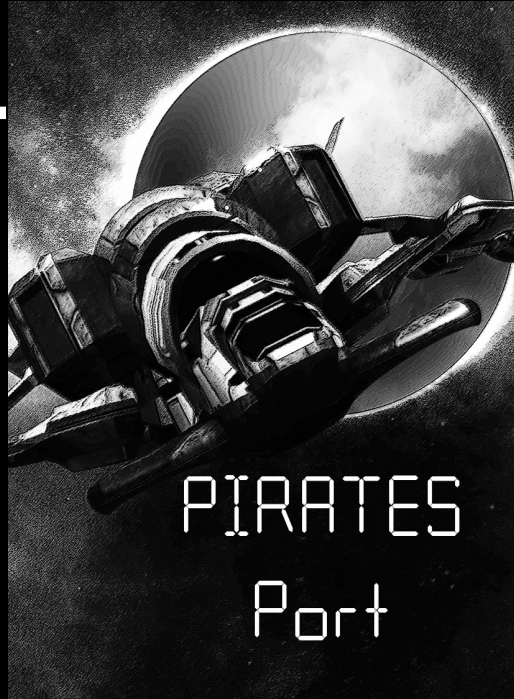




1 

P3

Skill

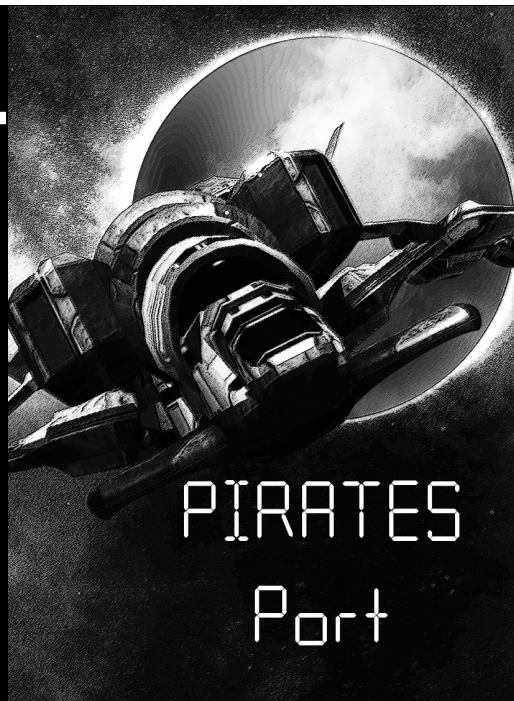


PIRATES
Port

1 

P1

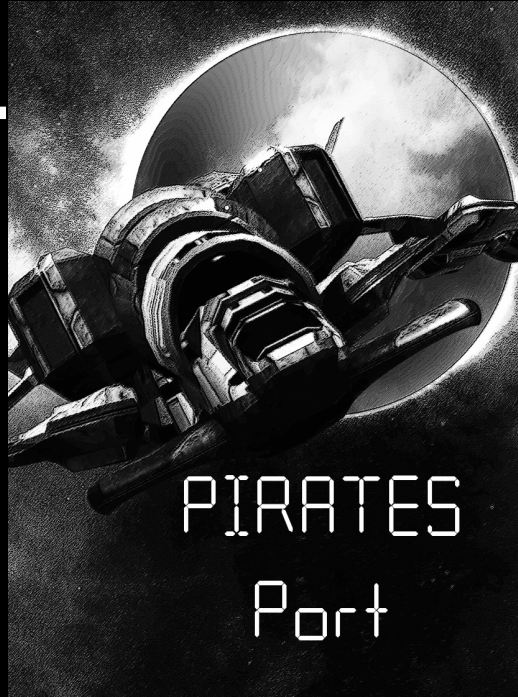
Money



PIRATES
Port

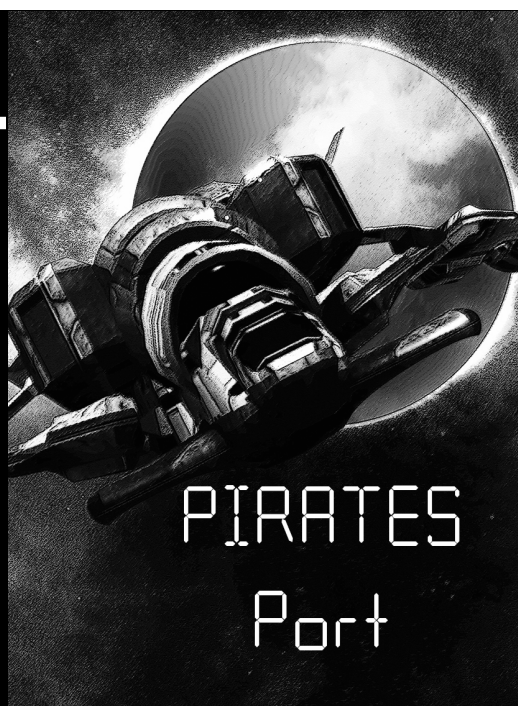
1  P1

Money



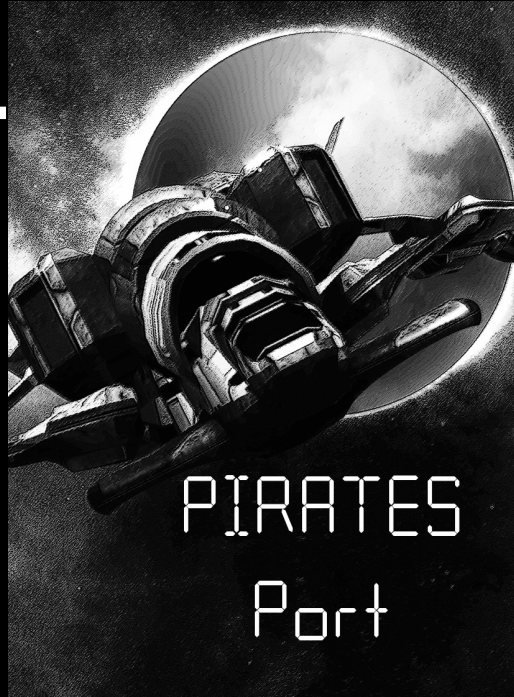
1  P2

Money



1  P2

Money

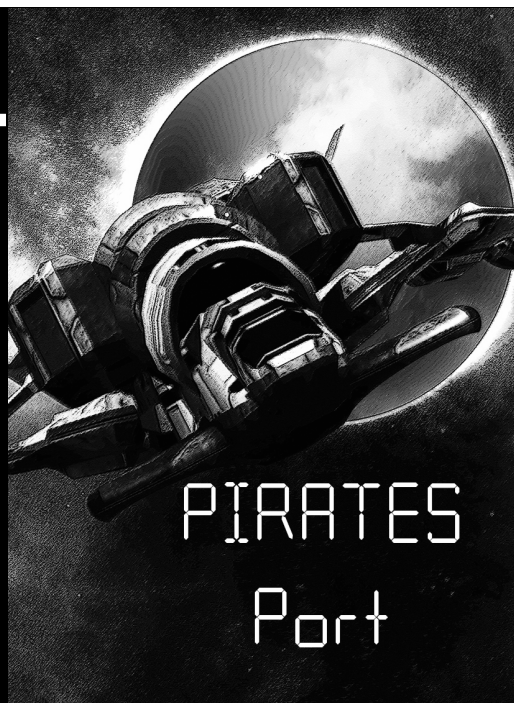


PIRATES
Port

EMP



There is no way to escape
the EMP!



PIRATES
Port

Mission: WEAPONS *

COMPLETE



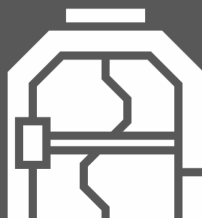
COST:  12 



Use a combination of twelve skill and coins to take out the guns

Mission: PORT *

COMPLETE



COST:  7



Use seven cards in your hand to open a port on the pirate ship

Mission: COMMS *

COMPLETE



COST:  6



Use six skill to take down the communication systems

Mission: COM

COMPLETE



COST:  5 



Spend five skill to take down the communication systems

Missions: ENGINES *

COMPLETE



COST:  6



Spend six coins to knock out the engines

Missions: ENGINES

COMPLETE



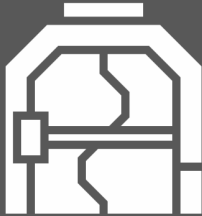
COST:  4 



Spend five coins to disable the engines

Mission: PORT *

COMPLETE



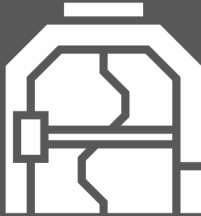
COST:  7



Use seven cards in your hand to open a port on the pirate ship

Mission: PORT

COMPLETE



COST:  3



Acquire three cards this turn to access the pirate ship port

Mission: Control

COMPLETE



COST:  14 



Use a combination of fourteen skill and coins to take full control of the ship

Mission: COMMS *

COMPLETE



COST:  6



Use six skill to take down the communication systems

Mission: Self-Aware

COMPLETE



COST:  10



You become self-aware after spending ten coins

Missions: ENGINES *

COMPLETE



COST:  6



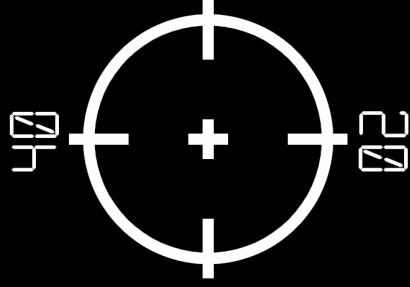
Spend six coins to knock out the engines

10



0

30



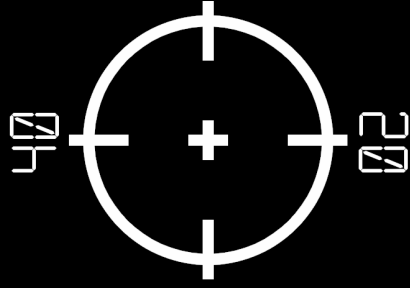
SCORE 50

10



0

30



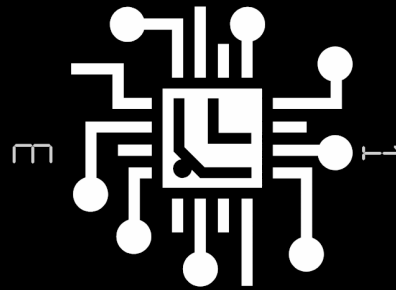
SCORE 50

SCORE

9
8
7
6
5
4
3
2
1

ALARM 0

AI



Score when a player cannot
deal with any events

2



SCORE

9
8
7
6
5
4
3
2
1

RULES

<https://pp.webdesk.me/rules.html>



EXTRAS

<https://pp.webdesk.me/>



SANS

<https://www.sans.org/>

