

port:1010

1 HIT

Persistent Malware

Obfuscated code saved to the Common Log
File System



PIRATES PORT
COUNTERATTACK



port:1010

2 HIT

Signed Driver

Signed Razer mouse driver privilege
escalation



PIRATES PORT
COUNTERATTACK



port:1010



Browser Plugin

Malicious Chrome extension supply chain attack



PIRATES PORT COUNTERATTACK



port:1010



Malicious Driver

Malicious driver deployed for keyboard input interception



PIRATES PORT COUNTERATTACK



port:1010

5 HIT

New Service

Persistence using Windows service disguised as EDR updater



PIRATES PORT
COUNTERATTACK



port:1010

6 HIT



Cloud Bucket

Data exfiltration through public cloud storage bucket



PIRATES PORT
COUNTERATTACK



port:1010



7 HIT

New User Added

New user assetmg created with administrator access



PIRATES PORT COUNTERATTACK



port:2472



1 HIT

Cloud Metadata

Cloud access through Instance Metadata Service exfiltration



PIRATES PORT COUNTERATTACK



port:2472



2 HIT

MFA Bypass

Office 365 MFA bypass using named location access



PIRATES PORT
COUNTERATTACK



port:2472



3 HIT

Watering Hole

Redirected to malicious website through Facebook Messenger



PIRATES PORT
COUNTERATTACK



port:2472

4 HIT

Cloud Account

Endpoints compromised through O365 Ruler payload delivery



PIRATES PORT
COUNTERATTACK



port:2472

5 HIT

Credential Stuffing

Citrix internal network access through reused credentials



PIRATES PORT
COUNTERATTACK



port:2472



6 HIT

Web Shell

Persistent access to web server with isolated code



PIRATES PORT COUNTERATTACK



port:2472



7 HIT

Malicious Kubelet

Kubernetes takeover with malicious kubelet deployment



PIRATES PORT COUNTERATTACK



port:3800

1 HIT

Fake Installer

Gain access through a fake installer



PIRATES PORT COUNTERATTACK



port:3800

2 HIT

O365 Macro

Command execution through O365 Excel document macro



PIRATES PORT COUNTERATTACK



port:3800



3 HIT

Sysmon Reporting
Malicious PowerShell invocation detected



PIRATES PORT COUNTERATTACK



port:3800



4 HIT

Shadow Copy
Access protected SAM database using
Volume Shadow Copy



PIRATES PORT COUNTERATTACK



port:3800



5 HIT

Password Audit

DPAT reveals systemic password selection exposure



PIRATES PORT COUNTERATTACK



port:3800



6 HIT

Sinkhole Domain

Malicious activity identified through a sinkhole DNS response



PIRATES PORT COUNTERATTACK



port:3800



7 HIT

Log Analysis

SIEM logging analysis identifies APT activity



PIRATES PORT COUNTERATTACK



port:4545



1 HIT

Persistent Malware

Obfuscated code saved to the Common Log File System



PIRATES PORT COUNTERATTACK



port:4545



2 HIT

Signed Driver

Signed Razer mouse driver privilege escalation



PIRATES PORT COUNTERATTACK



port:4545



3 HIT

Browser Plugin

Malicious Chrome extension supply chain attack



PIRATES PORT COUNTERATTACK



port:4545



4 HIT

Malicious Driver

Malicious driver deployed for keyboard input interception



PIRATES PORT
COUNTERATTACK



port:4545



5 HIT

New Service

Persistence using Windows service disguised as EDR updater



PIRATES PORT
COUNTERATTACK



port:4545



6 HIT

Cloud Bucket

Data exfiltration through public cloud storage
bucket



PIRATES PORT COUNTERATTACK



port:4545



7 HIT

New User Added

New user assetmgt created with administrator
access



PIRATES PORT COUNTERATTACK



port:5600

1 HIT



Cloud Metadata

Cloud access through Instance Metadata Service exfiltration



PIRATES PORT COUNTERATTACK



port:5600

2 HIT



MFA Bypass

Office 365 MFA bypass using named location access



PIRATES PORT COUNTERATTACK



port:5600



3 HIT

Watering Hole

Redirected to malicious website through
Facebook Messenger



PIRATES PORT
COUNTERATTACK



port:5600



4 HIT

Cloud Account

Endpoints compromised through O365 Ruler
payload delivery



PIRATES PORT
COUNTERATTACK



port:5600



5 HIT

Credential Stuffing

Citrix internal network access through reused credentials



PIRATES PORT COUNTERATTACK



port:5600



6 HIT

Web Shell

Persistent access to web server with isolated code



PIRATES PORT COUNTERATTACK



port:5600

7 HIT



Malicious Kubelet

Kubernetes takeover with malicious kubelet deployment



port:6834

1 HIT



Fake Installer

Gain access through a fake installer



PIRATES PORT COUNTERATTACK



PIRATES PORT COUNTERATTACK



port:6834

2 HIT

O365 Macro

Command execution through O365 Excel
document macro



PIRATES PORT
COUNTERATTACK



port:6834

3 HIT

Sysmon Reporting

Malicious PowerShell invocation detected



PIRATES PORT
COUNTERATTACK



port:6834



4 HIT

Shadow Copy

Access protected SAM database using
Volume Shadow Copy



PIRATES PORT
COUNTERATTACK



port:6834



5 HIT

Password Audit

DPAT reveals systemic password selection
exposure



PIRATES PORT
COUNTERATTACK



port:6834



6 HIT

Sinkhole Domain

Malicious activity identified through a sinkhole
DNS response



PIRATES PORT
COUNTERATTACK



port:6834



7 HIT

Log Analysis

SIEM logging analysis identifies APT activity



PIRATES PORT
COUNTERATTACK





exposed

PORT:1010

PIRATES PORT
COUNTERATTACK



Exposed
Port



exposed

PORT:2472

PIRATES PORT
COUNTERATTACK



Exposed
Port



exposed

PORT:3800

PIRATES PORT
COUNTERATTACK



Exposed
Port



exposed

PORT:4545

PIRATES PORT
COUNTERATTACK



Exposed
Port



exposed

PORT:5600

PIRATES PORT
COUNTERATTACK



Exposed
Port



exposed

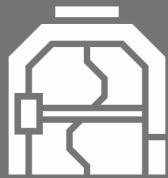
PORT:6834

PIRATES PORT
COUNTERATTACK



Exposed
Port

1



win to
infiltrate

PORT:1010

PIRATES PORT
COUNTERATTACK



PORT

2



wins to
infiltrate

PORT:2472

PIRATES PORT
COUNTERATTACK



PORT

3 wins to
infiltrate

PORT:3800



PIRATES PORT
COUNTERATTACK



PORT

4 wins to
infiltrate

PORT:4545



PIRATES PORT
COUNTERATTACK



PORT

5 wins to
infiltrate
PORT:5600

PIRATES PORT
COUNTERATTACK



6 wins to
infiltrate
PORT:6834

PIRATES PORT
COUNTERATTACK

