Background

MAYDAY PAYMENTS

Mayday Payments are a global financial institution that has a small to medium sized targetable attack surface comparable to similar financial companies.

Target

The target for this assessment is the corporate office in the UK as this is the primary record processing location. Mayday Payments do operate in other regions through subsidiaries and partnerships and have regional controls around data protection and data sharing, processing and transmission.

Deployment

Mayday Payments have a well-funded and appropriately staffed security team that have been empowered to secure the company. Due to sensitive payment data, network segmentation is implemented, and only specific groups have access. All data is encrypted at rest and stored within MongoDB clusters.

Scenario

You have been tasked with performing a simulated attack in line with Threat Actor (TA) Tactics, Techniques and Procedures (TTPs) provided within the document. The TA assigned to this scenario is: **AGGRESSIVE ORANGE**.

The goal for this scenario is to demonstrate vulnerabilities in the payment submission process that Mayday Payments operate for customers. Once access has been obtained the objective is to gather intelligence about various processes and procedures in use at Mayday Payments and exfiltrate fictitious samples of the identified information.

Goals of the scenario:

- Gain initial access into Mayday Payments via a customer portal
- Demonstrate weaknesses within the customer data transfer.
- Identify detection capabilities within the Mayday Payments environment.
- Measure exposure and access to internal sensitive data.
- Ensure the other relevant TTPs are executed

Detection

Mayday Payments have experienced previous breaches and have implemented a range of controls and detection mechanisms as part of the remediation plan.

TTP	Title	Description
T1082	System Information Discovery	Common Windows utilities will be detected
T1110	Password Spraying	Account Lockouts have been implemented
T1575	PSExec Lateral Movement	PSExec Service creation will be detected
T1562.001	Impair Controls: Disable or Modify Tools	AV is configured in detect mode throughout the estate

Web Server Hardening

A recent audit identified that a lack of application control was a significant issue and therefore this has been a focus for the internal security team.

Active Directory Attacks

Mayday Payments have a long-standing Active Directory environment, and this has been a challenge to maintain internally over the last few years.

Service Permissions

Service permissions issues were identified on several machines and the third-party software company have been advised.

Credential Management

User password management has historically been poor although central processes have been implemented and Mayday Payments request this as an area of review.

Anti-Virus Exclusion Rules

Finally, the on-host Anti-Virus solution created significant noise and therefore the internal teams have reduced false positives by allowing certain business processes. Mayday Payments want assurance that this has not reduced the security of the device as a result.

Threat Actor TTPs

AGGRESSIVE ORANCE has been known to use the following TTPs, some of which are marked as part of the exam, but all should be considered.

TTP	Title	Description
T1071.001	Application Layer Protocol	AGGRESSIVE ORANGE has used HTTP and HTTPS for C2 communications.
T1505.003	Web Shell	AGGRESSIVE ORANGE has used a web shell for persistence
T1555.004	Credentials from Password Stores:	AGGRESSIVE ORANGE has gathered credentials from the Windows Credential Manager tool.
T1005	Data from Local System	AGGRESSIVE ORANGE RPC backdoors can upload files from victim machines.
T1562.001	Impair Defences: Disable or Modify Tools	AGGRESSIVE ORANGE has used an AMSI bypass, which patches the in-memory amsi.dll to bypass Windows antimalware products.
T1069.001	Permission: Local Groups	AGGRESSIVE ORANGE has used “net localgroup” and “net localgroup Administrators” to enumerate group information, including members of the local administrators group.
T1090.001	Internal Proxy	AGGRESSIVE ORANGE has compromised internal network systems to function as a proxy to forward traffic to C2.
T1518.001	Security Software Discovery	AGGRESSIVE ORANGE has obtained information on security software, including security logging information that may indicate whether their malware has been detected.
T1007	System Service Discovery	AGGRESSIVE ORANGE surveys a system upon check-in to discover running services and associated processes using the tasklist /svc command.
T1078.003	Valid Accounts: Local Accounts	AGGRESSIVE ORANGE has abused local accounts that have the same password across the victim’s network.

Data

Domains

Domain Name	Source
mayday.payments	Various
mayday.payments	Email header
mayday.onmicrosoft.com	Azure Tenant
vpn.mayday.payments	Various
labsolutions.onmicrosoft.com	Azure Tenant
www.mayday.payments	DnsDumpster
dev-srv-01.external.mayday.payments	Certificate Transparency Logs
portal.mayday.payments	Pastebin
vpn.mayday.payments	DnsDumpster
sspr.mayday.payments	DnsDumpster
www2.mayday.payments	DnsDumpster
dev.mayday.payments	Pastebin
ext-dev-access.mayday.payments	Certificate Transparency Logs
mail.mayday.payments	DnsDumpster
customers.mayday.payments	DnsDumpster