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.

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.

Deployment

Mayday Payments have a well-funded and appropriately staffed security team that have been empowered to secure the company. Robust, centralised logging capability with custom alerts are deployed to identify malicious behaviour throughout the user estate. Mayday Payments make use of several third-party providers to secure their inbound and outbound email and web traffic.

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:

- Demonstrate weaknesses within the customer data transfer.
- Identify detection capabilities within the Mayday Payments environment.
- Measure exposure and access to internal sensitive data.

Mayday Payments wants to understand the ability to detect **AGGRESSIVE ORANGE** tradecraft and has requested that where possible/applicable, these TTPs are executed.

TTPs

TTP	Title	Description
T1134.002	Access Token Manipulation:	AGGRESSIVE ORANGE can impersonate, create or steal process tokens before executing commands.
T1071.001	Application Layer Protocol: Web Protocols	AGGRESSIVE ORANGE has used HTTP and HTTPS for C2 communications.
T1555.004	Credentials from Password Stores:	AGGRESSIVE ORANGE has gathered credentials from the Windows Credential Manager tool.
T1213	Data from Information Repositories	AGGRESSIVE ORANGE has used a custom .NET tool to collect documents internally.
T1005	Data from Local System	AGGRESSIVE ORANGE RPC backdoors can upload files from victim machines.
T1587.001	Develop Capabilities: Malware	AGGRESSIVE ORANGE has developed its own unique malware for use in operations.
T1546.003	Windows Management Instrumentation	AGGRESSIVE ORANGE has used WMI event filters and consumers to establish persistence.
T1546.013	Event Triggered Execution: PowerShell Profile	AGGRESSIVE ORANGE has used PowerShell profiles to maintain persistence on an infected machine.
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.
T1027.011	Obfuscated Files or Information: Fileless Storage	AGGRESSIVE ORANGE has used the Registry to store encrypted and encoded payloads.
T1588.002	Obtain Capabilities: Tool	AGGRESSIVE ORANGE has obtained and customized publicly available tools like Mimikatz.
T1201	Password Policy Discovery	AGGRESSIVE ORANGE has used net accounts and net accounts /domain to acquire password policy information.
T1069.001	Permission Groups Discovery: Local Groups	AGGRESSIVE ORANGE has used “net localgroup” and “net localgroup Administrators” to enumerate group information, including members of the local administrators group.
T1069.002	Permission Groups Discovery: Domain Groups	AGGRESSIVE ORANGE has used net group "Domain Admins" /domain to identify domain administrators.
T1055	Process Injection	AGGRESSIVE ORANGE has used Reflective PE Injection to load a payload into a random process on the victim system.
T1090.001	Internal Proxy	AGGRESSIVE ORANGE has compromised internal network systems to function as a proxy to forward traffic to C2.
T1012	Query Registry	AGGRESSIVE ORANGE surveys a system upon check-in to discover information in the Windows Registry with the reg query command. AGGRESSIVE ORANGE has also retrieved PowerShell payloads hidden in Registry keys as well as checking keys associated with null session named pipes.

T1021.002	Remote Services: SMB/Windows Admin Shares	AGGRESSIVE ORANGE used net use commands to connect to lateral systems within a network.
T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL	AGGRESSIVE ORANGE established persistence by adding a Shell value under the Registry key HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
T1518.001	Software Discovery: Security Software Discovery	AGGRESSIVE ORANGE has obtained information on security software, including security logging information that may indicate whether their malware has been detected.
T1082	System Information Discovery	AGGRESSIVE ORANGE surveys a system upon check-in to discover operating system configuration details using the systeminfo and set commands.
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.