CyberProof®
A UST Company

Top 10 attack techniques financial organizations should monitor in 2024

Here is a table of the top 10 MITRE ATT&CK tactics that financial organizations should be most aware of, including the type of tactic, which type of financial organization should be most aware, and why their organization may be vulnerable.

1 Initial Access TA0001

Most Affected Financial Organizations	Banks, Investment Firms
Why	Attackers often target financial systems through phishing, exploiting public-facing applications, or other entry points to gain access (MITRE ATT&CK).
Relevant Techniques	Phishing (T1566) (MITRE ATT&CK) Exploit Public-Facing Application (T1190) (MITRE ATT&CK) Valid Accounts (T1078) (MITRE ATT&CK)

2 Execution TA0002

Most Affected Financial Organizations	Insurance Companies, Banks
Why	Execution tactics involve running malicious code on a system, often through scripts or exploitation of vulnerabilities (MITRE ATT&CK) .
Relevant Techniques	Command and Scripting Interpreter (T1059) (MITRE ATT&CK) User Execution (T1204) (MITRE ATT&CK) Exploitation for Client Execution (T1203) (MITRE ATT&CK) Scheduled Task/Job (T1053) (MITRE ATT&CK)

3 Persistence TA0003

Most Affected Financial Organizations	Payment Processors, Retail Financial Services
Why	Persistence allows attackers to maintain access to systems, enabling prolonged exploitation of data (MITRE ATT&CK).
Relevant Techniques	Hijack Execution Flow (T1574) (MITRE ATT&CK) Boot or Logon Autostart Execution (T1547) (MITRE ATT&CK) Modify Authentication Process (T1556) (MITRE ATT&CK)

4 Privilege Escalation TA0004

Most Affected Financial Organizations	Banks, Credit Unions
Why	Attackers seek higher-level permissions to gain broader access and control within financial networks (MITRE ATT&CK).
Relevant Techniques	Exploitation for Privilege Escalation (T1068) (MITRE ATT&CK) Hijack Execution Flow (T1574) (MITRE ATT&CK)

5 Defense Evasion TA0005

Most Affected Financial Organizations	All Financial Sectors
Why	Techniques that allow attackers to avoid detection by security defenses are critical for stealth (MITRE ATT&CK) .
Relevant Techniques	Obfuscated Files or Information (T1027) (MITRE ATT&CK) Masquerading (T1036) (MITRE ATT&CK) Indicator Removal (T1070) (MITRE ATT&CK)

6 Credential Access TA0006

Most Affected Financial Organizations	Online Payment Platforms, Banks
Why	Financial institutions are prime targets for stealing account names, passwords, and other credentials (MITRE ATT&CK).
Relevant Techniques	Credential Dumping (T1003) (MITRE ATT&CK) Modify Authentication Process (T1556) (MITRE ATT&CK)

7 Discovery TA0007

Most Affected Financial Organizations	Investment Firms, Banks
Why	Attackers use discovery tactics to gather information about the environment, which is vital for planning further attacks (MITRE ATT&CK) .
Relevant Techniques	System Information Discovery (T1082) (MITRE ATT&CK) Account Discovery (T1087) (MITRE ATT&CK)

8 Lateral Movement TA0008

Most Affected Financial Organizations	Insurance Companies, Large Banks
Why	Lateral movement allows adversaries to move through a network, often to find sensitive data or further entrench themselves (MITRE ATT&CK).
Relevant Techniques	Remote Services (T1021) (MITRE ATT&CK)

9 Exfiltration TA0010

Most Affected Financial Organizations	Credit Unions, Investment Firms
Why	Attackers often aim to steal data, such as customer information or proprietary financial data, and exfiltration techniques facilitate this (MITRE ATT&CK).
Relevant Techniques	Exfiltration Over C2 Channel (T1041) (MITRE ATT&CK) Exfiltration Over Web Service (T1567) (MITRE ATT&CK)

10 Impact TA0040

Most Affected Financial Organizations	All Financial Sectors Impact
Why	Impact tactics focus on disrupting operations, such as through data destruction or manipulation, often leading to financial loss (MITRE ATT&CK).
Relevant Techniques	Data Encrypted for Impact (T1486) (MITRE ATT&CK) Data Manipulation (T1565) (MITRE ATT&CK)