Carbanak APT Attack on FinCore Financial Group (2018)

In 2018, FinCore Financial Group, a multinational financial institution, fell victim to a highly sophisticated cyber attack orchestrated by the Carbanak Advanced Persistent Threat (APT) group. Carbanak, infamous for targeting financial institutions worldwide, infiltrated FinCore's network to steal millions of dollars. FinCore offered a broad range of digital banking services to over 50 million customers, including cryptocurrency trading, mobile banking, and international payment systems. One Monday morning, FinCore's cybersecurity team observed irregular data flows between their internal systems, signaling a potential security breach. Further investigation revealed that Carbanak had compromised the bank's infrastructure weeks earlier and was orchestrating fraudulent wire transfers and ATM cash-outs in various countries.

Before executing their attack, Carbanak meticulously gathered intelligence on FinCore's internal operations. They researched the bank's infrastructure, software systems, and employees, identifying key personnel with access to critical financial systems. The attack began with Carbanak identifying specific weaknesses in FinCore's infrastructure. The bank's email security protocols were insufficiently hardened, allowing attackers to craft convincing spear-phishing emails that bypassed basic detection mechanisms. Carbanak also exploited vulnerabilities in FinCore's internal software systems—outdated and unpatched applications—enabling lateral movement within the network once initial access was achieved.

Carbanak used a malware strain in this attack, which modify parts of the code or encryption patterns to avoid detection, metamorphic malware completely rewrites its own code with each iteration. This made it particularly difficult for FinCore's antivirus solutions to detect and respond to the malware, as each instance of the malware appeared entirely unique. The malicious payload was embedded in a seemingly innocuous Microsoft Word document. When opened, the document executed a backdoor (RAT), allowing Carbanak to infiltrate the network.

The group then launched a targeted spear-phishing campaign, delivering the malicious document via email to several FinCore employees. Disguised as a legitimate message from a trusted business partner, the email was convincing enough to lead a finance department employee to open the attachment, unknowingly triggering the malware installation.

Once inside FinCore's network, Carbanak leveraged the RAT to obtain the employee's login credentials and escalated their privileges. They moved laterally across the network, infiltrating more critical systems and gaining access to sensitive financial databases. The attackers also installed backdoors on multiple systems, allowing them to maintain long-term, covert access to the bank's infrastructure.

For weeks, Carbanak operated undetected, using encrypted communication channels to control compromised systems remotely. They blended their activities with normal network traffic to evade detection, accessing customer transaction records and the bank's internal ATM control systems.

The Carbanak backdoor was highly sophisticated. After the malware was installed, it established encrypted communication channels with Carbanak's remote C2 servers. The attackers used these channels to issue commands to compromised machines and exfiltrate data, all while evading detection by security monitoring tools. The C2 servers would regularly change IP addresses and domains, further obfuscating the attack's origins. This allowed the attackers to continuously control FinCore's infrastructure remotely, the group executed their attack, initiating fraudulent wire transfers through FinCore's SWIFT payment network, moving millions to offshore accounts. Simultaneously, they remotely triggered ATMs in different countries to dispense cash to accomplices, or "mules."

When FinCore's investigation uncovered the full extent of the breach, the damage was staggering. Over $30 million had been stolen, and the attackers had accessed sensitive customer data, including transaction histories. While no immediate evidence of data exfiltration was found, the potential for future misuse loomed. The attack caused severe financial and reputational harm, forcing FinCore to compensate affected customers and significantly upgrade its cybersecurity defenses.

Actions Taken by FinCore Financial Group:

1. **Action-1:**
    - FinCore immediately isolated and shut down the compromised servers, especially those handling wire transfers and ATM operations. They disconnected external access to prevent further manipulation of financial systems.
    - The team applied security patches to the transaction processing systems and initiated a thorough audit to identify other vulnerabilities.
2. **Action-2:**
    - The bank implemented stronger encryption for all critical data and introduced multi-factor authentication (MFA) for both internal employees and high-risk financial transactions.
    - They adopted a Zero Trust Architecture, segmenting the network to prevent attackers from moving laterally within the system.
3. **Action-3:**
    - FinCore's cyber insurance policy covered a portion of the financial losses incurred during the attack, helping to offset the damage caused by the fraudulent transactions.
4. **Action-4:**
    - Customers were informed about the breach, and the bank compensated all those affected by fraudulent transactions. Free credit monitoring services were also provided to protect customers from potential identity theft or fraud.
5. **Action-5:**
    - The company enhanced its employee training programs, focusing on phishing awareness and how to spot social engineering tactics, ensuring employees could recognize potential threats.
6. **Action-6:**

- FinCore worked with law enforcement agencies and cybersecurity experts to track down the Carbanak group, while ensuring full compliance with regulatory reporting requirements to avoid further penalties.

7. **Action-7:**
   - A public statement was issued to reassure customers and stakeholders, detailing the steps taken to secure the bank's systems and warning that any future attacks would be met with legal action.

Question 2. In context of the case study, identify the following: [5 marks]

		Rubric
Asset:	FinCore's financial systems, customer data, and transaction processing infrastructure.	clearly mentioned: 1, ambiguous: 0.5, ZERO otherwise
Risk:	The risk of financial loss	clearly mentioned: 1, ambiguous or if only operational disruption: 0.5, ZERO otherwise
Threat Agent:	The **Carbanak APT Group**, a cybercriminal organization targeting financial institutions.	**1/0**
Threat:	Fraudulent wire transfers, ATM cash-outs, and potential data exfiltration (optional: leading to monetary loss and compromised customer data.)	**1 marks for any two of these, 0.5 for only one of these or Ambiguity, ZERO otherwise**
Vulnerability:	Outdated and unpatched internal software, insufficient email security, and lack of advanced detection mechanisms	**1 marks for any two of these, 0.5 for only one of these or Ambiguity, ZERO otherwise**
Exploit:	Spear-phishing email delivering a malware-laden Word document and exploiting syst em vulnerabilities to infiltrate FinCore's network.	**1 for both of these, 0.5 for anyone of these, ZERO otherwise**

Question 3. List five strategies organizations can use to manage or mitigate risks, each with a brief description. [5 marks]

Rubric: (0.5 for Name,
0.5 for Description, ZERO if ambiguous or incorrect)

Sr. #	Name	Description (Use only the provided space)

1	Risk avoidance	- involves identifying the risk but not engaging in the activity
2	Acceptance	- risk is acknowledged but no steps are taken to address it
3	Risk mitigation	- the attempt to address the risks by making risk less serious
4	Deterrence	- understanding the attacker and then informing him of the consequences of his actions
5	Transference	- transferring the risk to a third party

Question 4. For each of the actions taken by Global Bank, identify which risk management strategy was used: [7 marks]

Rubric: (
0.5 for correct strategy,

0.5 for correct description,

ZERO otherwise)

Actions	**Strategy**
Action-1	**Risk Mitigation:** Isolating and patching compromised systems reduces the threat's impact and limits the attack.
Action-2	**Risk Mitigation:** Implementing stronger encryption, MFA, and Zero Trust architecture to limit attack potential.
Action-3	**Risk Transference**: Using cyber insurance to offset financial losses from the attack.
Action-4	**Risk Mitigation**: Accepting responsibility for the breach, compensating affected customers, implemented free credit monitoring services to protect customers against identity theft.
Action-5	**Risk Avoidance**: Enhancing employee training reduces the likelihood of successful phishing attacks.
Action-6	**Deterrence**: Cooperating with law enforcement to pursue attackers sends a strong message and discourages future attacks.
Action-7	**Deterrence**: Issuing a public statement warning of legal action acts as a deterrent to other potential attackers.

Question 5: Map the key events in the case study to the relevant seven stages of a typical Cyber-Kill-Chain. [7 marks]

Stage in Attack Cyber-kill Chain	**Event Description**	**Rubic**

Reconnaissance	Carbanak researched FinCore's internal operations, infrastructure, and key personnel.	1 for all three of these, 0.5 for any two of these, Zero otherwise
Weaponization	Carbanak crafted a malicious Microsoft Word document embedded with a RAT (Remote Access Trojan).	1/0
Attack Delivery	Spear-phishing emails containing the malware-laden document were sent to FinCore employees.	1/0
Exploitation	An employee opened the document, executing the malware and providing initial access to the network.	1 for correct, 0.5 for ambiguous, ZERO otherwise
Installation	The RAT installed itself on FinCore's systems, establishing a foothold and setting up backdoors.	1/0
Command and Control	Carbanak used encrypted communication channels to remotely control compromised systems via C2 servers.	1/0
Actions on Objectives	Carbanak initiated fraudulent wire transfers and ATM cash-outs, stealing over $30 million.	1/0

Question 6: List five capabilities of the Carbanak backdoor used in the attack along with a brief description. [5 marks]

Rubric:
0.5 for correct capability identification (may use a matching phrase),
0.5 for correct unambiguous description

Sr. #	Capability	Description
1	key logging	Records all keystrokes entered on a victim's device, allowing attackers to steal sensitive data like passwords and PINs.
2	Desktop video capture	Captures video or screenshots of the victim's desktop activity, providing insight into the user's operations and data.
3	VNC (Virtual Network Computing)	Enables remote control of the victim's computer, allowing attackers to manipulate the system as if they were physically present.
4	HTTP form grabbing,	Intercepts and captures data entered into web forms, such as usernames, passwords, and other sensitive details submitted over HTTP.

5	file system management	Gives attackers the ability to browse, read, write, and delete files on the victim's computer, facilitating the exfiltration of sensitive data or the manipulation of critical files.
6	file transfer	Allows attackers to upload or download files to and from the victim's system, enabling data theft or the introduction of additional malware.
7	TCP tunneling	Enables attackers to encapsulate network traffic through a secure tunnel, bypassing firewall and network restrictions.
8	HTTP proxy	Allows the compromised system to act as a proxy for routing malicious traffic through the victim's network, masking the attacker's true origin.
9	OS destruction	Provides the capability to damage or destroy the operating system, rendering the victim's system unusable.
10	Outlook data theft	Steals data from Microsoft Outlook, including emails, contacts, and attachments, which may contain sensitive information.
11	and reverse shell.	Grants attackers command-line access to the victim's system, allowing remote execution of commands as if locally accessing the system.

Question 7: Mention the mutation type of malware they used in the attack, along with reason. [1 mark]

Rubric: 0.5 for Type, 0.5 for correct reason.

Mutation Type	**Reason**
Metamorphic Malware	The malware rewrote its own code during each iteration, making detection by antivirus tools difficult.