Name : Khunt Yash R.

Domain : Cyber Security Intern

Company : Extion InfoTech

Yash Khunt

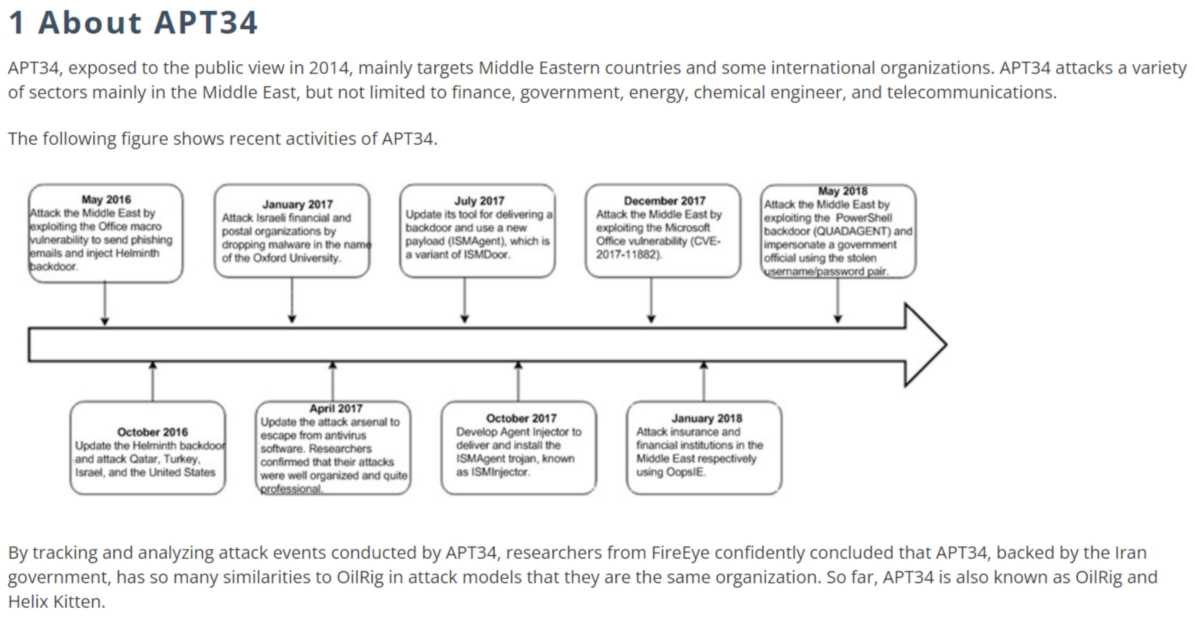
Investigation of a Data Breach

Report: Investigation of a Data Breach Attributed to APT34

Introduction

This report presents an investigation into a data breach incident attributed to APT34, a sophisticated Iranian cyber-espionage group known for targeting various sectors, including financial institutions, government agencies, and energy companies. The breach was discovered during a routine security audit at a fictional financial institution, ABC SecureBank. The investigation aims to uncover the techniques used by APT34, analyze the tools they employed, and provide recommendations for mitigating such threats in the future.

Overview of APT34



1 About APT34

APT34, exposed to the public view in 2014, mainly targets Middle Eastern countries and some international organizations. APT34 attacks a variety of sectors mainly in the Middle East, but not limited to finance, government, energy, chemical engineer, and telecommunications.

The following figure shows recent activities of APT34.

May 2016
Attack the Middle East by exploiting the Office macro vulnerability to send phishing emails and inject Helminth backdoor.

October 2016
Update the Helminth backdoor and attack Qatar, Turkey, Israel, and the United States

January 2017
Attack Israeli financial and postal organizations by dropping malware in the name of the Oxford University.

April 2017
Update the attack arsenal to escape from antivirus software. Researchers confirmed that their attacks were well organized and quite professional.

July 2017
Update its tool for delivering a backdoor and use a new payload (ISMAgent), which is a variant of ISMDoor.

October 2017
Develop Agent Injector to deliver and install the ISMAgent trojan, known as ISMInjector.

December 2017
Attack the Middle East by exploiting the Microsoft Office vulnerability (CVE-2017-11882).

January 2018
Attack insurance and financial institutions in the Middle East respectively using OopsIE.

May 2018
Attack the Middle East by exploiting the PowerShell backdoor (QUADAGENT) and impersonate a government official using the stolen username/password pair.

By tracking and analyzing attack events conducted by APT34, researchers from FireEye confidently concluded that APT34, backed by the Iran government, has so many similarities to OilRig in attack models that they are the same organization. So far, APT34 is also known as OilRig and Helix Kitten.

APT34, also known as "OilRig" or "OsiRis," is a cyber-espionage group believed to be affiliated with the Iranian government. APT34 is known for its persistent and targeted attacks, often leveraging social engineering, phishing campaigns, and custom malware to infiltrate networks and exfiltrate sensitive data.

Key Characteristics:

- **Target Sectors:** Government, financial services, telecommunications, energy, and critical infrastructure.
- **Geographical Focus:** Middle East, North America, and Europe.
- **Primary Objective:** Cyber-espionage, intelligence gathering, and disruption.

Breach Discovery

The breach at ABC SecureBank was identified when unusual network traffic was detected during a routine audit. Initial analysis indicated that the attackers had gained unauthorized access to the internal network, potentially compromising sensitive customer data, including names, account numbers, and transaction history.

Techniques and Tools Used by APT34

1. Initial Access: APT34 typically employs spear-phishing emails to deliver malicious payloads. These emails often appear legitimate, targeting specific individuals within an organization. The attackers craft messages to lure victims into clicking on malicious links or downloading infected attachments.

- **Techniques:** Spear-phishing, Social Engineering

  - **Spear-Phishing**

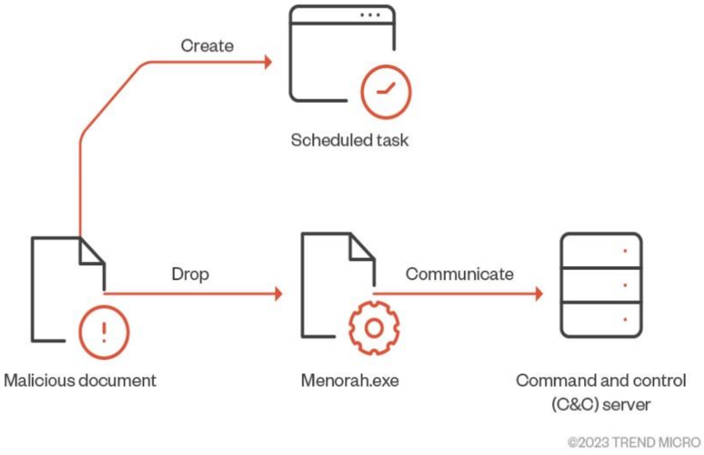
    Description: Spear-phishing is a targeted email attack in which the attacker impersonates a trusted entity to deceive the recipient into divulging confidential information or executing malicious code. APT34 has been known to use spear-phishing emails as an initial entry vector.

Execution: APT34 often sends emails with malicious attachments or links that, when opened, execute malicious scripts. These emails are typically tailored to the recipient, often appearing as legitimate business communications or government correspondence.

Impact: Spear-phishing can lead to unauthorized access to sensitive information, credentials, or the installation of malware on the target's system.

Example Tools:

- **Custom Scripts:** APT34 uses tailored scripts within their spear-phishing emails to download additional malware or to execute commands on the victim's system.



©2023 TREND MICRO

- **Tools:** Custom phishing frameworks, PowerShell-based scripts

2. Exploitation of Vulnerabilities: Once inside the network, APT34 often exploits known vulnerabilities in software or misconfigurations in the target's systems to escalate their privileges. This allows them to gain deeper access to the network.

- **Techniques:** Exploiting unpatched vulnerabilities, Privilege escalation

- **Tools:** Exploitation frameworks (e.g., Metasploit), Custom scripts

```
       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 >
```

3. Lateral Movement: APT34 is known for its ability to move laterally across compromised networks. They often use legitimate administrative tools to avoid detection, leveraging compromised credentials to access other systems within the network.

- **Techniques:** Credential dumping, Lateral movement using legitimate tools
- **Tools:** Mimikatz (for credential harvesting), PsExec (for lateral movement)

○ **Credential Harvesting**

Description: Credential harvesting involves the collection of usernames, passwords, and other authentication data to gain unauthorized access to systems and networks. APT34 utilizes several methods to harvest credentials, often following successful spear-phishing attacks.

Execution: APT34 typically uses phishing pages, keyloggers, and man-in-the-middle (MITM) attacks to collect credentials. Once harvested, these credentials are used to gain deeper access into networks.

Impact: Harvested credentials can provide APT34 with access to sensitive systems, allowing them to move laterally within the network, escalate privileges, and exfiltrate data.

Example Tools:

- **CredoMap:** A phishing toolkit used by APT34 to harvest credentials through fake login pages.
- **Keyloggers:** Custom keyloggers designed to capture keystrokes and transmit them back to the attacker.

- **Web Shell Deployment**

Description: Web shells are malicious scripts that enable remote administration of a compromised web server. They allow attackers to execute commands, upload and download files, and pivot to other systems within the network.
Execution: APT34 deploys web shells on compromised servers to maintain persistent access. These web shells are typically uploaded via vulnerabilities in web applications or through previously harvested credentials.
Impact: Web shells allow APT34 to maintain a foothold in the network, even after initial indicators of compromise have been detected and remediated.
Example Tools:

- **TwoFace:** A web shell used by APT34 to execute arbitrary commands on compromised servers and to exfiltrate data.
- **China Chopper:** A widely used lightweight web shell that provides attackers with a user-friendly interface for controlling compromised servers.

4. Command and Control (C2): After establishing a foothold, APT34 sets up command and control channels to maintain communication with the compromised network. They use various techniques to disguise this traffic as legitimate, making detection more difficult.

- **Techniques:** Encrypted C2 communications, Use of DNS tunnelling

  - **DNS Tunneling**

Description: DNS tunneling is a technique that uses the Domain Name System (DNS) protocol to transmit data between the victim and the attacker. This technique can be used to exfiltrate data or to establish command and control (C2) channels.

Execution: APT34 uses DNS tunneling to hide their malicious traffic within legitimate DNS queries and responses, making it difficult for traditional security measures to detect.

Impact: DNS tunneling allows APT34 to exfiltrate data covertly and to maintain communication with compromised systems, even in highly monitored environments.

Example Tools:

- **dnscat2:** An open-source tool used for DNS tunneling, enabling APT34 to maintain stealthy communication channels.
- **IODINE:** A DNS tunneling tool that encapsulates data within DNS queries, making it difficult to detect and block.

- **Tools:** Custom C2 frameworks, PowerShell-based C2 channels
- **5. Data Exfiltration:** APT34 carefully exfiltrates data to avoid detection, often compressing and encrypting the stolen data before sending it to external servers controlled by the attackers. They might use cloud services, FTP, or even HTTP(S) traffic to exfiltrate data.
- **Techniques:** Data compression and encryption, Use of legitimate protocols for data exfiltration
- **Tools:** 7-Zip (for compression), Custom exfiltration scripts, FTP clients

- **Custom Malware**

  Description: APT34 has developed and deployed a range of custom malware tailored to their specific needs. These malware variants often have multiple capabilities, including data exfiltration, credential harvesting, lateral movement, and command execution.
  Execution: Custom malware is typically delivered through spear-phishing, drive-by downloads, or exploited vulnerabilities. Once deployed, the malware communicates with the attacker's C2 servers and executes the desired payload.
  Impact: Custom malware can provide APT34 with full control over compromised systems, enabling them to conduct long-term espionage, exfiltrate sensitive data, and disrupt operations.
  Example Tools:
  - **POWBAT:** A remote access trojan (RAT) used by APT34 for persistence, data exfiltration, and remote command execution.
  - **Webmask:** A modular malware framework that allows APT34 to execute various plugins for different stages of the attack lifecycle.

Forensic Analysis

The forensic analysis of the breach involved examining system logs, network traffic, and endpoint devices. Key findings include:

- **Compromised User Accounts:** Several employee accounts were found to have been compromised, likely through spear-phishing attacks.
- **Unusual Network Traffic:** Analysis of network traffic revealed the use of DNS tunneling for command and control communications.

- ### Network Traffic Analysis :

Description: Network traffic analysis involves capturing and inspecting network packets to identify suspicious activity, including communication with known malicious IP addresses or the use of DNS tunneling.

Tools:

- **Wireshark:** A widely used network protocol analyzer that captures and inspects the data traveling across the network. Wireshark can help identify malicious DNS queries, abnormal traffic patterns, and C2 communications.
- **Bro/Zeek:** A network monitoring tool that provides real-time analysis of network traffic, detecting anomalies and logging relevant information for further investigation.

Application: By analyzing network traffic, investigators can identify signs of DNS tunneling, unusual outbound connections, and the use of web shells for communication.

- **Malware Artifacts:** Custom malware associated with APT34, including backdoors and credential harvesters, was identified on several compromised systems.

- ### Digital Forensics

Description: Digital forensics involves the systematic collection, preservation, analysis, and presentation of digital evidence from compromised systems. This is crucial for understanding the breach, identifying the attackers, and collecting evidence for potential legal action.

Tools:

- **Autopsy/Sleuth Kit:** A digital forensics platform used for examining file systems, recovering deleted files, and analyzing disk images. It is particularly useful for investigating compromised systems and uncovering traces of malware.

- **EnCase:** A comprehensive digital forensics tool used for acquiring, analyzing, and reporting on digital evidence. EnCase is often employed in large-scale investigations where multiple systems are involved.

Application: Digital forensics allows investigators to recover and analyze artifacts left by APT34, including malware binaries, log files, and evidence of credential harvesting or data exfiltration.

- **Malware Analysis**

Description: Malware analysis is the process of examining the malicious software deployed by the attackers to understand its functionality, behavior, and impact on the compromised system.

Tools:

- **IDA Pro:** A powerful disassembler and debugger used for analyzing the assembly code of malware. IDA Pro helps reverse-engineer malware to uncover its inner workings.
- **Cuckoo Sandbox:** An automated malware analysis system that runs suspicious files in a controlled environment to observe their behavior and generate detailed reports.

Application: Malware analysis helps investigators understand the specific capabilities of the tools used by APT34, including how they were able to maintain persistence, exfiltrate data, and evade detection.

- ### Log Analysis

Description: Log analysis involves reviewing system and network logs to trace the attackers' actions, identify compromised accounts, and detect unauthorized changes to systems and configurations.
Tools:

- **Splunk:** A log management and analysis tool that aggregates logs from various sources, enabling investigators to search, analyze, and visualize data in real-time.
- **ELK Stack (Elasticsearch, Logstash, Kibana):** A suite of tools for searching, analyzing, and visualizing log data. The ELK Stack is often used to detect patterns and correlations in large datasets.

Application: Log analysis helps identify the timeline of the breach, the methods used by APT34 to escalate privileges and move laterally, and any data that may have been exfiltrated.

- ### Endpoint Detection and Response (EDR)

Description: EDR tools are used to monitor endpoints (such as workstations, servers, and mobile devices) for signs of malicious activity. They provide visibility into the actions of attackers and can help contain the breach.
Tools:

- **CrowdStrike Falcon:** An EDR platform that provides real-time monitoring, detection, and response capabilities for endpoints. It uses behavioral analysis and threat intelligence to detect and respond to attacks.
- **Carbon Black:** An EDR solution that continuously records and analyzes endpoint activity to detect and respond to threats. It allows investigators to track the attackers' movements and gather evidence.

Application: EDR tools help identify compromised endpoints, trace the attackers' movements, and contain the breach by isolating affected systems and stopping malicious processes.

Mitigation and Recommendations

1. Strengthening Email Security:

- Implement advanced email filtering solutions to detect and block spear-phishing emails.
- Conduct regular employee training on recognizing and reporting phishing attempts.

2. Patch Management:

- Ensure all systems are up-to-date with the latest security patches.
- Regularly audit systems for vulnerabilities and apply patches promptly.

3. Network Segmentation:

- Implement network segmentation to limit the movement of attackers within the network.
- Use firewalls and access controls to restrict access to sensitive areas of the network.

4. Monitoring and Detection:

- Deploy advanced intrusion detection and prevention systems (IDPS) to monitor for signs of lateral movement and unusual network activity.
- Use endpoint detection and response (EDR) tools to detect and respond to malicious activities on endpoints.

5. Incident Response Planning:

- Develop and regularly test an incident response plan that includes procedures for responding to breaches and communicating with stakeholders.
- Ensure that logs are securely stored and regularly reviewed to detect potential security incidents.

Conclusion :

The data breach at ABC SecureBank attributed to APT34 highlights the advanced techniques and persistent nature of this threat actor. By exploiting human vulnerabilities and system weaknesses, APT34 was able to infiltrate the network and potentially exfiltrate sensitive data. This incident underscores the importance of a multi-layered security approach, regular employee training, and robust incident response planning to defend against such sophisticated threats.

The investigation of a data breach attributed to APT34 requires a comprehensive understanding of their tools and techniques, as well as the use of advanced investigation tools to uncover and mitigate the breach. By employing a combination of network traffic analysis, digital forensics, malware analysis, log analysis, and EDR, investigators can effectively trace the attackers' activities, assess the damage, and take steps to prevent future incidents.

APT34's use of spear-phishing, credential harvesting, web shell deployment, DNS tunneling, and custom malware highlights the importance of maintaining robust security measures and continuously monitoring for signs of compromise. By learning from this investigation, organizations can strengthen their defenses against advanced persistent threats and reduce the risk of future breaches.