Adobe Cloud File Share Phishing Campaign Redirects Users to Malicious Domains

TL;DR

A phishing campaign is using Adobe Cloud file-sharing links to deliver malicious content. The emails appear legitimate and ***may*** *come from spoofed or compromised government-related accounts.*

Users open an Adobe file that contains a link to a malicious site designed to steal credentials or deliver further malicious content.

Overview

There is an active phishing campaign using Adobe Cloud file-sharing links to deliver malicious documents. The emails **may** originate from legitimate sources and **may** involve spoofed or compromised government email accounts.

The email includes a link to an Adobe Cloud-hosted file along with a passcode to access it. This makes the message look credible and helps it bypass security controls. Once the user opens the file, the PDF contains a link that directs them to a malicious external site. The initial link points to a legitimate domain, which reduces suspicion and increases the chance of user interaction. This activity aligns with known phishing campaigns that use trusted cloud services to deliver malicious content and move users to credential harvesting pages.

If successful, the attacker can capture user credentials, gain access to email or cloud accounts, and use that access to move further into the environment or send additional phishing emails from a trusted account. Organizations should block the domains involved and stress the importance of user awareness around unexpected file-sharing requests.

Aspire Protects

- Be cautious of Adobe documents that require a passcode and then prompt you to click a link
- Confirm the sender through a separate method before accessing documents
- Email and Web Security:
  - Block known malicious domains such as `cabocesorg[.]top`
  - Monitor and restrict high-risk TLDs such as `.top` where appropriate
- Require MFA for email and cloud accounts
- Monitor for unusual login activity following user interaction

- Review logs for Adobe file access followed by redirects to external domains

***Note**: Aspire thanks Ryan Rose from NERIC for bringing this to the CTI team's attention.*

TTPs to Watch

Initial Access

- Phishing: Spearphishing Link [T1566.002] – The attacker may send an email containing an Adobe Cloud link that directs the user to attacker-controlled content.

- Phishing: Spearphishing via Service [T1566.003] – The attacker may use a legitimate cloud service to deliver phishing content and increase trust in the link.

Defense Evasion

- Masquerading [T1036] – The attacker may present the email as coming from a trusted source to reduce suspicion.

Credential Access

- Input Capture: Web Portal Capture [T1056.003] – The attacker may capture user credentials through a fake login page after redirecting the user.

IoCs

Email Domain

- sender[.]sender@**nysed[.]gov**
  - *Observed sender domain in this campaign. This domain belongs to the New York State Education Department, a legitimate U.S. government organization. The full sender address has been reduced to the domain to avoid exposing a potentially legitimate user. Emails included Adobe Cloud file-sharing links and may have been spoofed or sent from compromised accounts. Use caution with unexpected messages from this domain.*

Domains

- cabocesorg[.]top
  - *Phishing domain used for credential harvesting. Observed in sandbox analysis hosting fake login pages – Joe Sandbox*

- newyorkstateeducationdepartment[.]cabocesorg[.]top
  - *Malicious subdomain impersonating a government education entity; observed hosting phishing content in sandbox analysis – Joe Sandbox*

Targeted Industries

This phishing campaign targets organizations that rely on email communication and cloud-based file sharing for daily operations.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Adobe Acrobat Scam Emails: Insights From Our Threat Team - Hoxhunt

Docs-Shared Adobe Acrobat Sign phishing scam - Search Engine Optimisation Marketing SEO

Adobe Acrobat Sign Impersonators Use Customized… | Abnormal AI

What Is the Adobe Phishing Attack Impersonation - GreatHorn

Phishing via Adobe Acrobat: A Cloud Abuse Technique - Netskope