U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0293

ADOBE ACROBAT SIGN - PHISHING EMAILS

DATE ISSUED: 20th March 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

The info-stealing malware Redline is distributed through phishing emails using legitimate Adobe Acrobat Sign services. The malware is capable of harvesting account credentials, cryptocurrency wallets, credit card details, and other sensitive information.

BREAKDOWN

Security researchers at Avast discovered a new trend in cybercrime that exploits Adobe Acrobat Sign platform to send malicious emails. Adobe Acrobat Sign is a cloud-based e-signature service that allows the user to send, sign, track, and manage signature processes using a browser or mobile device. Threat actors register with the service and exploit it to send malicious emails hosted on Adobe's servers. The email contains a link to a website that requests visitors to solve a CAPTCHA to add legitimacy and then serve them a ZIP archive that includes a copy of the Redline information stealer. The malware is inflated to 400 MB which helps to avoid anti-virus scan detection.

REMEDIATION STEPS

- Use a password manager that stores credentials in an encrypted vault.
- Activate multi-factor authentication (MFA) to secure your accounts. This adds an additional layer of protecton if the credentials have been stolen.
- Educate users on how to spot phishing and social engineering emails and what to do with them in your organisation.
- Avoid opening ZIP files and attachments unless they are from a known trusted source and are expected.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/adobe-acrobat-sign-abused-to-push-redline-info-stealing-malware/