CIRT.GY Guyana National Computer Incident Response Team

AL2025_47 New MatrixPDF toolkit turns PDFs into phishing and malware lures (October 02nd , 2025)

Description

A new phishing and malware distribution toolkit called MatrixPDF has been discovered on cybercrime forums, enabling threat actors to transform ordinary PDF files into weaponized attack vectors that bypass email security filters and deliver malicious payloads. The toolkit allows attackers to augment legitimate PDF documents with malicious features including fake overlays, embedded JavaScript actions, blurred content, and interactive buttons that redirect victims to phishing sites or trigger malware downloads.

Attack Details

MatrixPDF is a builder-style toolkit that converts legitimate PDF documents into weaponized attack vectors by importing real files and augmenting them with malicious overlays, clickable prompts, embedded JavaScript, blurred content and customizable payload URLs for phishing or malware distribution. Because the generated PDFs contain no binaries or executable attachments—only scripts and external linksthey can evade many email security gateways and antivirus scanners that rely on signature- or attachment-based detection; in testing, MatrixPDF files render normally in Gmail's web viewer without triggering phishing warnings because the malicious content is only fetched after user interaction. Attackers commonly use two delivery methods: phishing via PDF preview, where recipients who preview the file in Gmail see blurred content with a convincing "Open Secure Document" overlay that redirects them to phishing pages or malware downloads when clicked (an action that appears user-initiated and thus bypasses some scanning controls), and JavaScript payload delivery, where downloaded PDFs opened in desktop PDF readers that support document-level scripting automatically attempt to contact attacker-controlled URLs to fetch payloads relying on social engineering to overcome reader warnings about external connections. The toolkit makes social engineering easy by producing professional-looking "protected" prompts, realistic formatting, shortened benign-looking URLs (for example, ln.run), and other trust-building elements to increase click-through rates. By splitting stages across email, web browsers and external hosting, MatrixPDF also creates a multi-stage attack chain that defeats defenses which examine each component in isolation. Primary targets are Gmail users, corporate email systems and organizations that routinely exchange PDFs, while desktop users whose PDF readers permit JavaScript execution are especially vulnerable to automatic payload retrieval.

Remediation

MatrixPDF poses a significant threat to Guyana's public and private sector organizations as PDF files are widely trusted and commonly used for official communications, contracts, invoices, government documents, and business correspondence. With Guyana's ongoing digital transformation initiatives and increasing reliance on email-based communications across government agencies, financial institutions, and businesses, this toolkit's ability to bypass standard email security makes it particularly dangerous. Organizations in Guyana's critical sectors including banking, energy, telecommunications, and government ministries should prioritize implementing the remediation measures below, as successful phishing attacks can lead to credential theft, financial fraud, data breaches, and unauthorized access to sensitive systems.

- **User Awareness Training:** Educate users about PDF-based phishing attacks. Train them to be suspicious of PDFs with blurred content, unexpected "Open Secure Document" prompts, or requests to click buttons or links within PDF files received via email.
- **Email Security Enhancement:** Deploy AI-driven email security solutions that analyze PDF structure, detect suspicious overlays and fake prompts, identify embedded JavaScript, and detonate embedded URLs in sandbox environments before delivery to user inboxes.
- **PDF Reader Configuration:** Configure PDF readers (Adobe Acrobat, etc.) to disable automatic JavaScript execution by default and require explicit user approval for any external connections or script execution attempts.
- **Link Analysis:** Implement URL filtering and analysis tools that inspect shortened URLs and external links embedded in PDF files before allowing users to access them. Block access to newly registered or suspicious domains.
- **Email Gateway Policies:** Configure email gateways to quarantine or flag PDF files containing JavaScript, external URL references, or interactive elements for additional security review before delivery.
- **Endpoint Protection:** Deploy endpoint detection and response (EDR) solutions capable of monitoring PDF reader behavior, detecting suspicious JavaScript execution, and blocking unauthorized outbound connections initiated by PDF readers.
- **Verify Sender Authenticity:** Train users to verify the legitimacy of email senders before opening PDF attachments, especially those claiming to contain "secure" or "protected" documents requiring special actions to view.
- **Multi-Factor Authentication:** Implement MFA on all accounts to mitigate the impact of credential theft from phishing attacks that may use MatrixPDF-generated documents.
- **Incident Response:** If compromise is suspected, immediately disconnect affected systems, reset credentials for potentially compromised accounts, scan for malware, and review PDF reader logs for evidence of malicious JavaScript execution or unauthorized network connections.
- The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Abrams, L. (2025, September 30). New MatrixPDF toolkit turns PDFs into phishing and malware lures. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/new-matrixpdf-toolkit-turns-pdfs-into-phishing-and-malware-lures/?&web_view=true

- Varonis. (2025, September 30). MatrixPDF Puts Gmail Users at Risk with Malicious PDF Attachments. Retrieved from Varonis Security Research. https://www.varonis.com/blog/matrixpdf