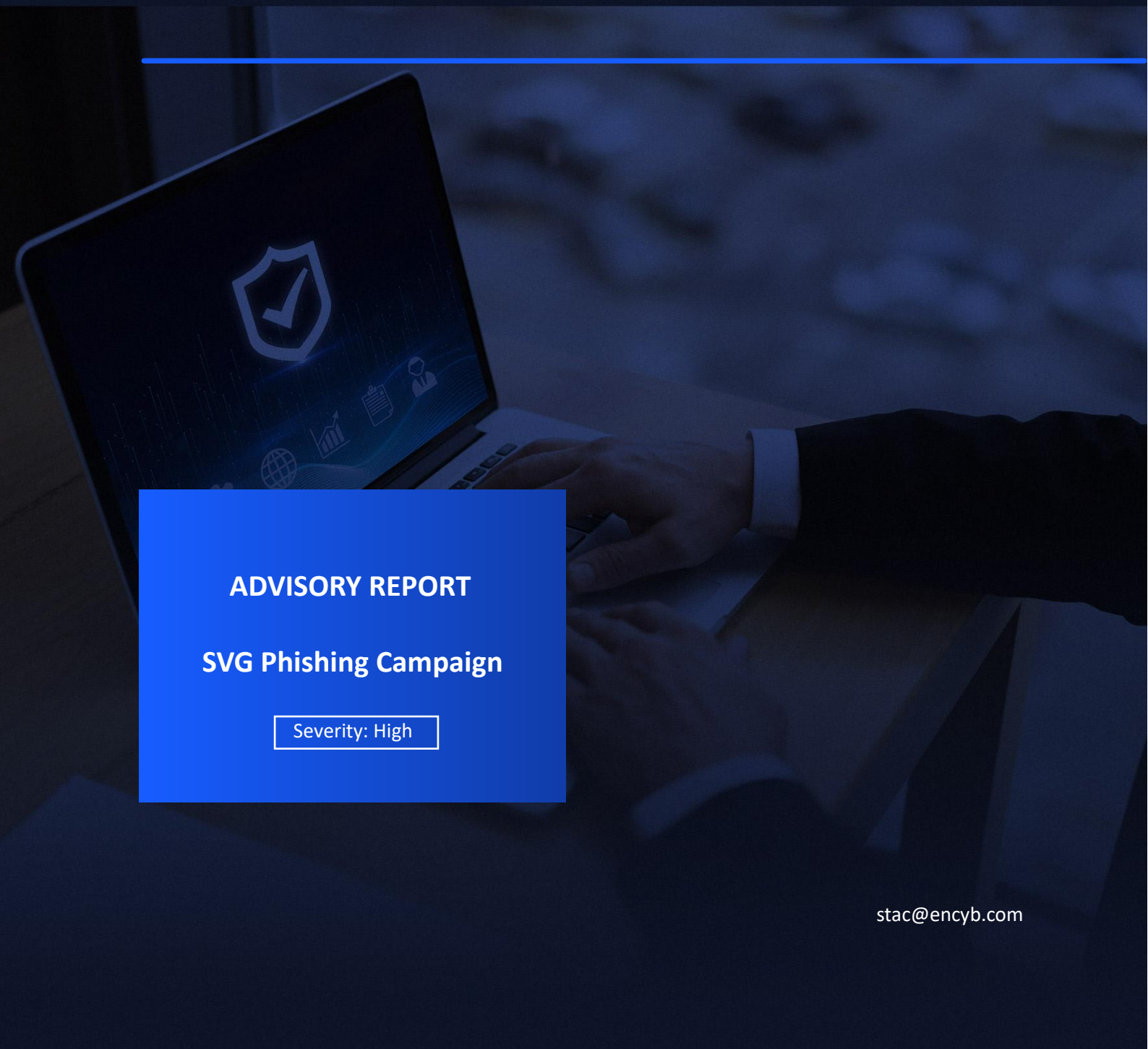
EnCyb

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.



ADVISORY REPORT

SVG Phishing Campaign

Severity: High

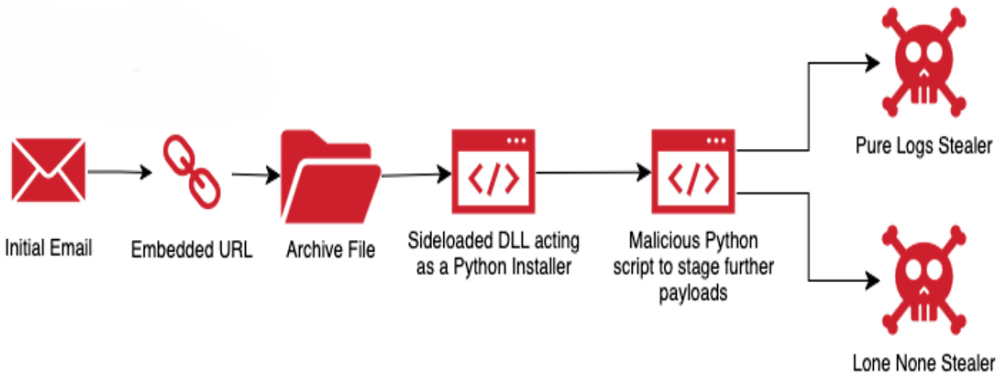
stac@encyb.com

OVERVIEW

Microsoft has identified a phishing campaign using malicious SVG (Scalable Vector Graphics) files disguised as PDFs or file-sharing notifications. These files contain hidden scripts that redirect users to CAPTCHA pages and then to fake login portals to steal credentials. The attack is notable for its likely use of AI (LLMs) to generate verbose, business-themed code that appears legitimate and evades detection, and for employing a self-addressed email tactic where the real targets are hidden in BCC. Although the campaign was limited and blocked, it highlights the growing sophistication of AI-driven phishing and the importance of strong email security and user awareness.

TECHNICAL DETAILS

- **Malware Type:** SVG-embedded JavaScript used to redirect victims to CAPTCHA and fake login pages for credential harvesting; potential secondary payloads include information stealers and RATs.
- **Delivery Vector:** Malspam emails with .svg attachments disguised as PDFs; self-addressed emails with real recipients in BCC; sometimes sent from compromised internal accounts.



- **Execution & Capabilities:** Executes inline JavaScript to perform browser fingerprinting, conditional redirects, and exfiltration of entered credentials; may download additional payloads.
- **Obfuscation Techniques:** LLM-style code with verbose, business-themed variable names and comments; CDATA sections, XML declarations, and encoded attributes to evade static detection.
- **Network & Detection Indicators:** Redirects to intermediate CAPTCHA and credential pages; fingerprinting query parameters (ua, tz, screen, lang); detectable via <script> tags in SVGs, unusual filenames, and self-addressed email patterns.
- **File Indicators:** SVG files contain <script> tags, <![CDATA[, or <?xml declarations; filenames often mimic PDFs (e.g., invoice.pdf.svg) and may have minimal legitimate graphics.
- **Endpoint / EDR Signals:** Browser processes are spawned by email clients when the SVG is opened; suspicious outbound HTTPS connections to new or low-reputation domains can indicate credential exfiltration.

TTP MAPPING

TACTICS	TECHNIQUES	ID
Initial Access	Phishing — Attachment (SVG disguised as PDF)	T1566.001
Execution	User Execution (opening/preview of attachment)	T1204
Execution	JavaScript execution in SVG (inline scripting)	T1059.007
Defence Evasion	Obfuscated files / verbose LLM-style obfuscation	T1027
Credential Access	Web-based credential harvesting (phishing landing page)	T1566
Command & Control	Exfiltration over C2 / HTTPS POST of harvested data	T1041
Lateral Movement	Use of valid accounts (reuse of harvested credentials)	T1078
Impact	Secondary delivery — download of additional payloads (info-stealers, RATs)	T1105

IMPACT

- Credential theft: Attackers can gain access to corporate email, cloud accounts, VPNs, and other critical systems using stolen usernames, passwords, or session cookies.
- Data exfiltration: Sensitive corporate information, intellectual property, financial records, and customer data may be stolen and sent to attacker-controlled servers.
- Lateral movement: Compromised credentials allow attackers to move across internal networks and access restricted or sensitive systems.
- Secondary malware deployment: Attackers may deliver additional malware, such as info-stealers, remote access trojans (RATs), or ransomware, increasing the overall impact and persistence.
- Operational disruption: Unauthorized access, malware activity, or system tampering can interrupt normal business operations, cause downtime and diverting resources to incident response.
- Financial loss: Organizations may face costs related to remediation, forensic investigation, recovery, and potential regulatory fines, as well as indirect losses from operational disruption.
- Reputational damage: Exposure of sensitive or customer data can harm the organization’s brand, erode client trust, and negatively affect partnerships or market position.
- Regulatory and compliance exposure: Breaches involving regulated data may trigger mandatory reporting, audits, and fines under laws like GDPR, HIPAA, or sector-specific regulations.

RECOMMENDATIONS

- Block or quarantine suspicious .svg attachments and files with mismatched MIME types; implement advanced phishing filters for self-addressed emails and spoofed senders.
- Educate employees about phishing tactics and simulate phishing exercises to reinforce safe email habits.
- Require MFA authentication for all critical accounts to reduce the impact of stolen credentials.
- Restrict execution of scripts from email attachments.
- Disable automatic preview of SVG files; enforce strict policies for opening attachments from untrusted sources.
- Keep browsers, email clients, and endpoints updated; limit macro/script execution in office documents.
- Periodically review user accounts and permissions.

REFRENCE

- Microsoft Flags AI-Driven Phishing: LLM-Crafted SVG Files Outsmart Email Security