केनरा बैंक Canara Bank

सिंडिकेट Syndicate

Advisory - 09

DATE: 26.05.2020

JavaRAT campaigns: Targeting Indian Financial Institutions

• Adwind JavaRAT / JsOutProx RAT campaign

- The campaign uses spear-phishing emails posing as either RBI or a large banking organization
- The email content may refer to new RBI guidelines or a transaction with detailed information in an attached zip/archive file which contains a malicious JavaScript / Javabased backdoors.
- Upon execution, the JavaScript / JAR file transforms into a Remote Admin Tool (JRat) which can perform keylogging, capturing screenshots, downloading additional payloads, and getting user account information
- The JAR has multi-layer obfuscation to make analysis harder and bypass detection from security tools.
- Both of these JavaRAT campaigns could potentially steal customer data from banks, along with important financial infrastructure details, create persistent backdoors for future use, planning fraudulent transactions or other cyber-attacks

• Safety Measures:

- Be cautious about opening any attachments or downloading files received via email , if source is unknown.
- Look for the sender email ID before you provide any confidential information.
- Do use a separate email accounts for personal use like shopping online, Social websites, etc.
- Don't reply to an e-mail or pop-up message that asks for personal or financial information.
- Never give out Personal Information over phone or to unsecured sites.
- In case of any incident contact hoisg@canarabank.com or ciso@canarabank.com

A V Rama Rao
General Manager

INFORMATION SECURITY SECTION, RISK MANAGEMENT WING