Are your Agency Bots up to no good?

By **Sarbari Gupta, Chief Executive Officer, Electrosoft Services, Inc.** - September 9, 2022

Federal agencies are rapidly embracing robotic process automation (RPA) technology to deploy "bots" or specially designed software programs that automate the performance of routine, repetitive tasks. The rationale is simple: bots deliver quantifiable task performance benefits in the form of vastly reduced human effort, cost and error rates. However, the very algorithms that make bots desirable can simultaneously introduce vulnerabilities into an agency's security posture.

CURRENT FEDERAL LANDSCAPE

According to the Federal RPA Community of Practice's recent report on the state of federal RPA, the first federal RPA application was deployed in 2017. Since that time, federal demand for RPA has only grown.

Among 65 federal RPA programs surveyed for the report, 49 were deploying bots, while 16 were exploring that possibility. The 49 reported FY 2020 automation deployment numbers that were2.5 higher than FY2019 levels. Moreover, existing and planned deployments were expected to create about 1.5 million hours of capacity that will allow federal employees to focus efforts on higher value work.

When it comes to IT security approvals, however, the survey reported that many federal agency programs employ "low level security and technology measures." The report sees this finding as expected, but it underscores the need not just to enhance security at the bot and

agency level but also to create common security and technology approaches across government.

KEY SECURITY CONSIDERATIONS

Specific security needs will depend on the federal agency, the system and the data handled by bots, but governmentwide governance practices will hold many tenets in common. Three over arching considerations include: identity and access management, security analysis, and security monitoring and forensics.

Identity and Access Management

Bots act as end-entities for transactions. Hence, they require identity credentials and privileges sufficient to perform the targeted functions. While managing the identities and privileges of bots would appear to be straightforward, it is not.

Bots frequently employ the identity authentication credentials of a human user. The Federal RPA Community of Practice survey put the number of bots either employing human user credentials or no credentials whatsoever at76 percent. Assigning human user privileges can yield access levels that far exceed those needed to perform a specific task, thereby violating the security principle of "least privilege." It also creates an accountability problem as it is impossible to attribute specific actions to the human user or the bot acting on behalf of that user. The hazards of no credentials are profound and self-evident.

Federal agencies need to assure that each bot or group of bots performing related functions operate using a unique identity and related authentication credentials. Then, each unique bot identity can be accorded the minimum privileges needed to perform its assigned task. Second, bots must be secured in a manner that they cannot be hijacked and used by malware on the network. Last, agencies must actively manage the lifecycle of bot identity credentials from creation until the identities can be disabled/deactivated.

Managing bot identities and privileges over their lifetime could add a heavy burden to agency Identity, Credential, and Access Management(ICAM) programs. Beyond establishing and implementing governance protocols, agencies will need to perform ongoing account/credential management and access enforcement functions. These tasks could be substantial given the proliferation of bots within many agencies.

There is dissonance between bot use and agency efforts to move toward multi-factor authentication (MFA) and zero trust. For example, it is difficult to implement MFA in bots. Given the undeniable benefits of bots, solving this dilemma will pose an important challenge for federal agencies.

Bot Security Analysis

Traditional applications employ code/scripts that can easily undergo static and dynamic security analysis using a variety of tools. Extracting the code/scripts from the proprietary

RPA tools used to build bots can be much more difficult, making analysis of their security properties a challenge.

Absent static and dynamic security analysis, agency IT environments face potential vulnerabilities because bots can browse different URLs and open email attachments. Without careful analysis of bot code, it is impossible to mitigate the risk of a bot browsing unsafe URLs or opening malware- laden attachments/documents.

Additionally, bots can gather, analyze and push out data. Without reviewing bot security architecture and code/script, agencies cannot assure that sensitive data is protected adequately either at rest or during transmission. Further, they cannot review the business workflow of the bot to ascertain whether potential security vulnerabilities exist.

Bot Security Monitoring and Forensics

When bots are actively deployed on agency network environments, it is essential that the actions of bots are monitored and tracked to ensure they comply with agency security policies and metrics. Thus, monitoring bot actions for security and privacy implications is vital. It necessitates the following considerations:

- Recording bot actions via detailed audit logs and analyzing the logs regularly to identify actual security incidents and impending security attacks.
- Analyzing bot activities in ways similar to analysis of privileged user actions and identifying advanced persistent threats (APTs) using bot credentials.
- Conducting forensic analysis of bot actions over time when a suspected or realized security incident occurs.

LEVERAGING LIMITLESS POTENTIAL

The benefits associated with bots are well documented, and their potential uses in the federal work environment appear limitless. Yet, safeguarding the security of government systems must remain uppermost. RPA demands a well-defined security approach that integrates time-tested principles with robust methodologies that consider the unique functions and features of bots.

Sarbari Gupta, Chief Executive Officer, Electrosoft Services, Inc.