Securing the new wave of non-human users

Juliette Rizkallah, SailPoint


Juliette Rizkallah

It is no secret that the advent of the digital age has spurred significant progress in businesses – particularly with the rising deployment of bots and artificial intelligence (AI) to boost efficiency in the workplace. But, as with most opportunities, there are challenges. And, unfortunately for businesses, fraudsters are not lagging behind when it comes to adopting these technological innovations to support their criminal efforts. As companies increasingly embed artificially intelligent 'workers' to help support operations, they are unwittingly exposing themselves to further risk if not properly secured, creating additional pathways for fraudsters to infiltrate.

To protect themselves from falling prey to hackers seeking to take advantage of early adopters of digital transformation, organisations must make sure their security measures keep pace with their innovation efforts. In the case of bots, they must effectively secure these non-human users in the same way that they secure their human users to eliminate potential risk.

"Organisations that have tens of thousands of customers can save a lot of time and money by automating these menial tasks. And that's not a bad thing, as long as these bots and their access are being appropriately governed and secured"

However, hackers are using these very same technologies to quicken the pace with which they launch attacks against organisations, with their sights set on breaching user accounts in new and innovative ways. As such, organisations must be prepared to not only embrace these innovations, but also to protect themselves should bots and AI be used against them. This article will explore the innovative ways that bots and AI can enable organisations, as well as the ways in which hackers will try to use these technologies to wreak havoc.

Digital transformation

Digital transformation is spurring new technology advances in the enterprise IT landscape. One of the most highly publicised of these technologies is the software bot, which is enjoying a wave of popularity within today's organisations. They are using bots to automate repetitive manual business and IT processes, allowing IT teams to offload monotonous, time-consuming tasks and focus on other priorities. This can be in the form of bot-driven virtual assistants, customer service chatbots, order fulfilment and travel booking for employees.

These bots are saving organisations both time and money as they seek to drive business efficiencies while keeping pace with digital transformation. For example, an enterprise can outsource order fulfilment to a bot that can work faster than a human, with potentially less error. Organisations that have tens of thousands of customers can save a lot of time and money by automating these menial tasks. And that's not a bad thing, as long as these bots and their access are being appropriately governed and secured. But given the tasks they are executing, these bots also have permissions that give them access to a variety of sensitive organisational data.

An organisation's users have become an increasingly bigger target for cyber attackers who see stolen user credentials as the proverbial 'keys to the kingdom.' In fact, the vast majority of data breaches, whether conducted by a cyber attacker from inside or outside of an organisation, involve the misappropriation of digital identities and their associated account credentials. Cyber attackers are seeing the value of exploiting valid user accounts to gain unauthorised access to sensitive systems and high-value personal and corporate data, often going undetected for hundreds of days. And with the new wave of software bots, hackers have even more valid user accounts to target, especially given that many organisations are not governing these software bots in the same way that they are with human identities.

Taming the bots

While the risk of unauthorised access cannot be completely eradicated, identity governance helps organisations regain control – enabling them to compare who has access to what, who should have access to what and what they are doing with that access. As organisations allow bots to have similar access as their human counterparts, they must also manage these non-human users in the same way as their human counterparts. As such, enterprises need to tightly govern the access that bots have to their systems, applications and data.

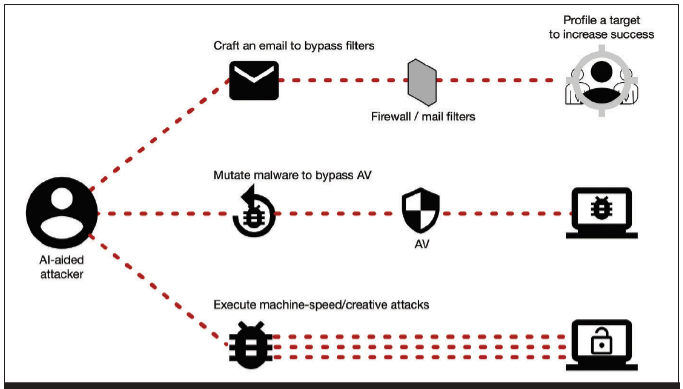
Often, this will mean treating bots in the same way as contractor-based identities, with policies that grant access only to the applications and data they need. It's also important to realise that bots have a lifecycle in the enterprise,

just like an employee or a contractor whose role may change or evolve as they move around the company. As such, a bot's lifecycle needs to be regularly reviewed, updated and ultimately decommissioned if the bot is no longer serving its purpose.

By extending identity governance programmes to include non-human users such as bots, IT teams can monitor application and data access, as well as strange user behaviours, to help search for any anomalies or potential breaches. Bringing software bots under the watchful eye of identity governance also makes it easier to control a bot should it become compromised.

With increasing regularity, companies are looking for 'break glass' functionality in their cyber security solutions. This means the company can take instant, targeted action in the event of a data breach, whether on site or working remotely. In the case of bots and other identities that have been compromised, this means immediately terminating an identity to shut off access to critical data and applications and re-provisioning access once it has been determined that a threat no longer exists. This functionality gives organisations the control they need to minimise the potential damage of a compromised identity, whether financial or reputational.

In the same way that a human employee has a line manager and access privileges, bots and their access to enterprise applications and data should be defined and governed on an ongoing basis. In case the bot identity is compromised, there should be systems and processes in place that would help disable or terminate its access to sensitive systems, files and documents immediately. This is not something that most enterprise identity programmes currently account for, but the tides are quickly shifting. At the end of the day, we need to ensure that all identities in the enterprise – human, or non-human software bots – have a well-defined role, with proper entitlements and governance of their access.



Commonly used ways to employ AI to aid malware attacks. Source: IBM.

Taking advantage of AI

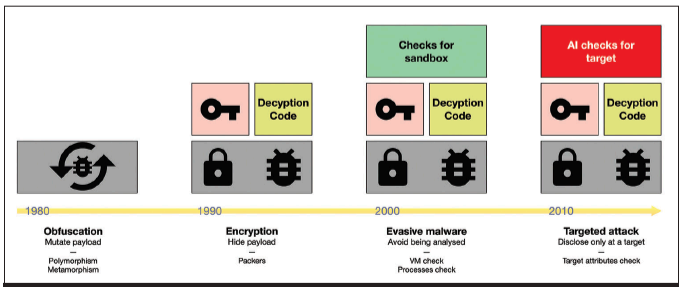
While organisations are increasingly using bots powered by AI to gain efficiencies, hackers are using these very same technologies to do untold damage. As with any other technological advancements, bots and AI are another opportunity for risk when harnessed by the wrong hands. Hackers are quick on the heels of organisations in the adoption of innovations like bots and AI – only they are using them to enhance their criminal abilities.

Bots and AI can be used for a variety of nefarious reasons and because of their ability to process large amounts of data with limited oversight necessary, their ill-effects can be exponentially detrimental to organisations. They can infiltrate datacentres or file rooms, learn confidential information and put organisations and their customers at great risk. In fact, a recent study found that when instituting a phishing scheme against humans, it was not the human hacker, but rather the AI-driven hacker that had the higher click-through rate and succeeded more often in converting malicious click-throughs into successful phishing attacks.[1,2]

Turning the AI tables

So, if AI is enabling hackers to penetrate computers at a faster rate than ever before, could this technology also be used to help secure organisations? Is it possible that the very technology threatening enterprise security could also be its new front line of defence?

As a security measure, AI's value proposition is appealing in various industries with a skills shortage and an ever-increas-



The evolution of malware concealment showing the application of 'locksmithing' in which the malware is encrypted – and thus hidden – and unlocked only in the right circumstances. Earlier versions of this were designed to hide malware from the sandbox environments used by researchers and anti-malware protections. In the current evolution, AI is used to determine whether the infected machine is the intended target. Source: IBM.

ing volume of security logs and alerts to analyse and react to. AI can help IT teams wade through thousands upon thousands of security alerts every day, alerting them to potential security threats and exposure points. With AI taking on the burden of sorting through the signal-to-noise ratio, IT teams can focus their efforts on being more effective at taking down those threats before the damage is done.

AI is a great example of a technology that, when applied to cyber security, can smartly advance IT efficiency and security. But what we have not fully considered is how this type of technology innovation may introduce new areas of exposure that hackers can use to their advantage. The more we innovate in cyber security, the more fuel to the proverbial fire we may be providing to cyber criminals.

Where do we go from here?

Bots and AI will not end the cyber war for good, simply because progress itself is actually fuelled from both sides of the law. In cyber security, innovation is critical in fending off the ever-evolving cyber criminals. But the truth is that hackers work just as quickly. As organisations continue to leverage new innovations like AI and bots, they must work to protect them too.

Enterprise IT teams must remain vigilant to prevent their organisations from becoming the next big data breach as hackers become ever more resourceful and 'less human' with malicious AI bots representing the 'dark side'. Or even better, organisations can fully embrace these new technologies to turn the tables on would-be bad actors, using these emerging technologies to enable their IT teams and secure their environments.

About the author

A marketing veteran with more than 20 years of experience, Juliette Rizkallah is responsible for articulating Sailpoint's company vision, product solutions, technology innovations and business purpose to customers, partners and media around the globe. She has held executive positions at a number of companies, including Oracle, CA, Business Objects-SAP and Check Point Software. She holds an MBA from Harvard Business School.

References

1. Stoecklin, Marc. 'DeepLocker: How AI Can Power a Stealthy New Breed of Malware'. SecurityIntelligence, IBM, 8 Aug 2018. Accessed Nov 2018. https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/.
2. Kirat, Dhilung; Jang, Jiyong; Stoecklin, Marc. 'DeepLocker – Concealing Targeted Attacks with AI Locksmithing'. BlackHat USA 2018. Accessed Nov 2018. www.blackhat.com/us-18/briefings/schedule/#deeplocker – -concealing-targeted-attacks-with-ai-locksmithing-11549.