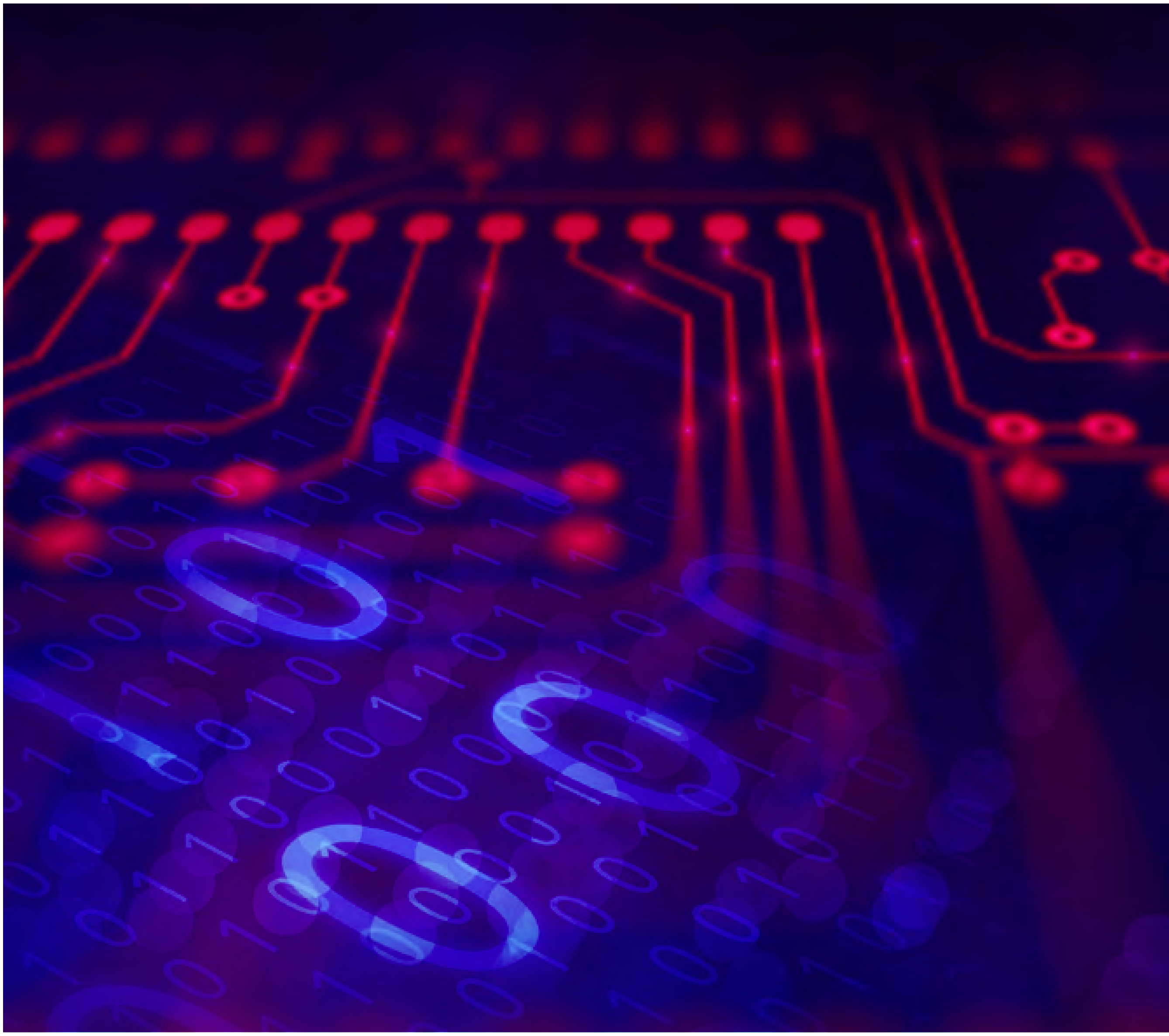
DARKReading RESEARCH

FEBRUARY 2022



Three Out of Four Attacks: Sophisticated Bots and What Enterprise Security is Missing

HUMAN

Executive summary

Over the past several years, bots have dramatically transformed the way we engage with the Internet, handling a dizzying array of online activities, including indexing large amounts of data and providing customer service functions. And while there are numerous positive outcomes of automation, bots can also have a negative side, wreaking havoc for businesses as well as their customers.

Previous research conducted in 2021 uncovered that cyber attackers using bots have increased the intensity of their efforts and are focusing on websites with a large number of visitors where there are marketing programs and incentives in place to drive traffic. Data from that survey showed that potentially vulnerable organizations often lacked the tools that provide the visibility needed to defend against bot attacks and scope out the impact of breaches. Most importantly, our findings suggested an educational and awareness gap across organizations regarding the capabilities of sophisticated bots.

Data from a new survey from Dark Reading and HUMAN Security which follows up on that earlier survey indicates that a significant majority of medium to large organizations recognize the value of bot management and understand the damage malicious bots can cause. Survey participants reported experiencing a variety of bot attacks (or suspected attacks) against their digital operations, including account takeovers and network disruptions. The most common incidents targeted site performance and customer accounts. However, our findings show that despite growing awareness about the sophistication of bot attacks, the vast majority of organizations are still not using the optimal tools for defense.

Key findings

This study, conducted among 100 cybersecurity and IT professionals at companies with 500 or more employees, found:

- During the last 12 months, organizations experienced, or believe they experienced, attacks that can pose major issues for their operations, including site slowdowns caused by overwhelming traffic (35%), credential stuffing (25%), account takeover (ATO) (21%), and content manipulation (20%).
- Organizations have a range of concerns about bot attacks: ATO (47%), site slowdowns caused by overwhelming traffic (37%), sensitive content scraping (30%), and credential cracking/brute force attacks (29%).
- Bot attacks bring economic and reputational consequences for targeted organizations, such as negative customer experience (47%), loss of revenue (46%), as well as implications for compliance, legal, shareholder value, and resource management (31%).
- Most organizations (81%) ranked protecting public-facing websites and applications from bot-driven attacks fraud and logic abuse among their top 10 priorities. However, in practice, just a quarter (24%) used bot management tools and only 7% used a specialized bot management solution.

Bots Create Chaos for Organizations and Customers

Just last year, in February 2021, a major streaming music provider was hit with a credential stuffing attack using login information harvested from a separate data breach. Once inside, the cybercriminals used their access to play certain songs and albums, helping artificially pump up their popularity and position on the digital charts. Attacks like this one are often carried out by sophisticated bots, which allow a criminal to scale up an operation quickly and efficiently.

Cybercriminals can deploy malicious, sophisticated bots in many ways, including distributing malware, launching ATO attacks, sending out spam messages, and generating fraudulent online clicks to artificially boost website traffic. As the Mirai attack of 2016 showed, the fact that attackers can sell or share successful bot tactics and code with others means they can expand a botnet's footprint exponentially, not to mention how much damage they can cause.

The increasing availability of bot-based tools and open-source building kits expanded the different types of attacks that can be launched. Misusing bots for malicious or fraudulent purposes is no longer merely a nuisance for organizations, but rather sophisticated attacks that can cause economic and financial impact on business operations.

For example, pandemic shoppers have used bots to beat supply chain challenges and snag hard-to-acquire game consoles or computer components. However, in August 2021, a major sneaker manufacturer saw a massive influx of bots targeting a high-profile release of new shoes, with some botmasters claiming to have scooped up more than 1,000 pairs of shoes for resale using so-called "sneakerbots." In addition, the California Community College system had to fend off an onslaught of fake student bot accounts in what appeared to be fraudulent COVID-19 relief grants and other financial aid.

The good news – There are now tools available to quickly detect, and often prevent, bot attacks.

In April 2021, HUMAN partnered with research firm ESG on a report showing that as organizations shifted to online-focused business operations, attackers doubled down and increased the frequency of bot-driven fraud and logic abuse.

> *Despite growing awareness about the sophistication of bot attacks, many organizations are still not using the optimal tools for defense.*

New research, conducted by Dark Reading in November 2021, extends this conversation to learn how organizations prioritize security and invest in solutions to detect and stop advanced attacks. In this survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, respondents held job titles such as CISO, Head of Information Security, and Security Architect.

Nearly half of survey respondents (48%) work at companies with more than 5,000 employees, and one-fifth work at companies with more than 50,000 employees. Participating industry sectors ran the spectrum. The top five were education and training (14%), banking and financial (12%), healthcare and medical (12%), government and defense (9%), and information and communication technology (8%).

Bots Impact Multiple Strategic Business Areas

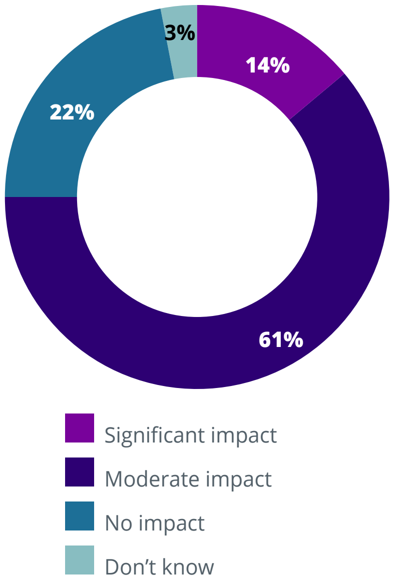
Attacks Can Create Obstacles for Successful Digital Transformation

Bot-driven cyberattacks have left their mark and fraudulent, revenue-threatening activities continue to be a concern. About three-quarters of respondents said that bot-driven attacks and fraudulent traffic have impacted their organization's digital transformation initiatives, with 61% reporting moderate and 14% significant impact **(Figure 1)**. A little over a fifth, or 22%, said there has been no impact to their digital transformation activities.

Figure 1.

Level of Impact of Bot-Driven Attacks on Digital Transformation Initiatives

How much of an impact have bot-driven attacks and fraudulent traffic had on your organization's digital transformation initiatives?



Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

When asked about attacks their organization experienced or may have experienced during the last 12 months, survey participants reported a variety of attack types. Respondents reported site slowdowns caused by overwhelming traffic (35%), credential stuffing (25%), and ATO attacks, in which attackers gained illegitimate access to existing accounts (21%). Respondents also reported experiencing other types of bot attacks, including sensitive content scraping (20%); content manipulation, such as generating fake or malicious user-generated content; (20%); and brute force/credentialing attacks (17%).

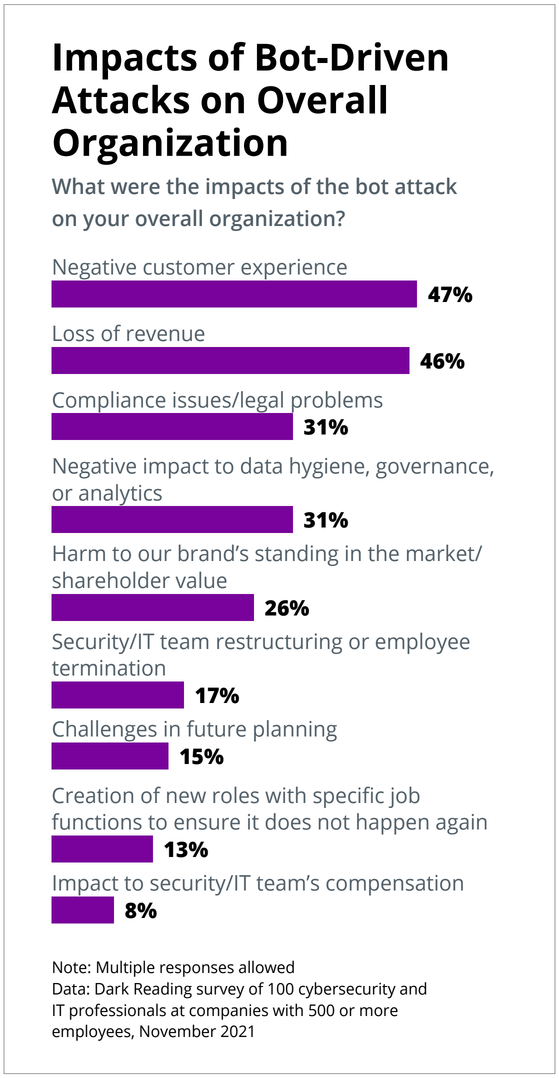
Increased Compliance Concerns Driven by Bots

Data security and privacy are major issues for organizations, especially with regulators taking interest in what is being done to safeguard consumer data. Respondents were asked about their level of concern about maintaining compliance with privacy and data regulations, such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA). Three-fourths expressed some level of concern over the regulations and their organization's ability to remain compliant (44% very concerned and 31% somewhat concerned). 31% of respondents (*in Figure 2*) said that sophisticated bots had *already* created legal or compliance concerns for them.

Sophisticated Bots Have a Negative Effect on Brand and Revenue

Bot attacks jeopardize the brand experience and ultimately impact the bottom line. According to respondents, the fallout can often lead to a negative customer experience (47%), loss of revenue (46%), as well as harm to the brand's standing in the market/shareholder value (26%) **(Figure 2)**.

Figure 2.



Impacts of Bot-Driven Attacks on Overall Organization

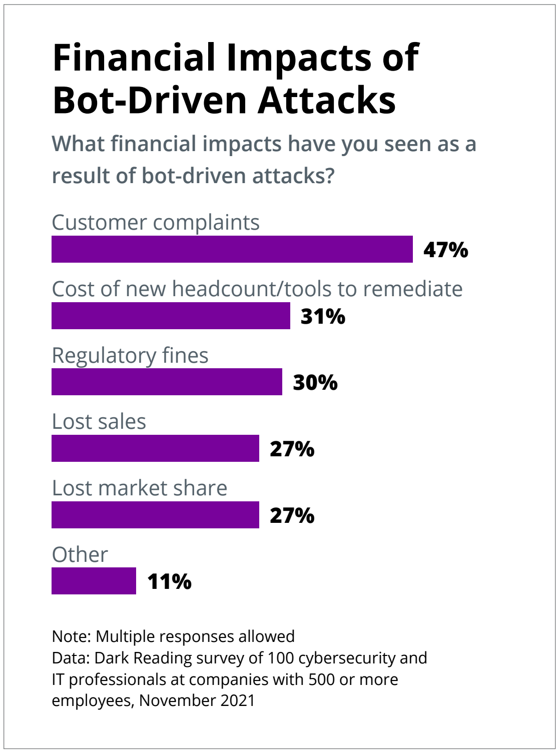
What were the impacts of the bot attack on your overall organization?

Note: Multiple responses allowed
Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

The economic impact of attacks has manifested as regulatory fines (30%) and loss of sales (27%) **(Figure 3)**. There is a recognition that bot attacks could compromise existing privacy and security controls and put an organization out of compliance.

The economic impact of attacks has manifested as regulatory fines (30%) and loss of sales (27%). There is a recognition that bot attacks could compromise existing privacy and security controls and put an organization out of compliance.

Figure 3.



Financial Impacts of Bot-Driven Attacks

What financial impacts have you seen as a result of bot-driven attacks?

Note: Multiple responses allowed
Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

> *Survey participants reported a variety of attack types, including site slowdowns (35%), credential stuffing (25%), and account takeover attacks (21%).*

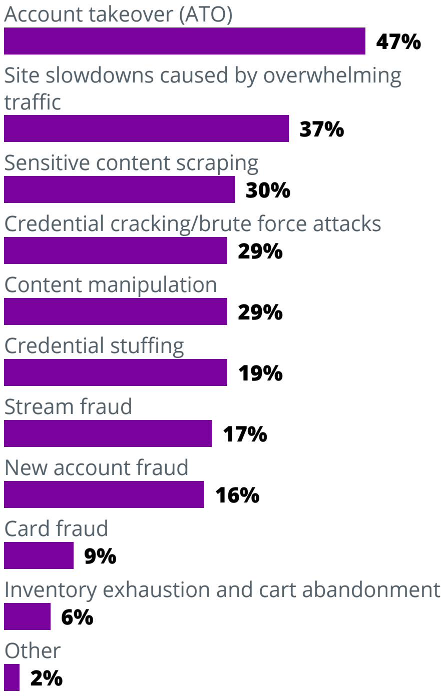
Bot Management Ranks High Among Organizational Priorities

Given the potential threat to strategic and financial goals, we set out to uncover how bot management ranked among organizational concerns. The majority of respondents (56%) placed bot management among their top 10 priorities. When the focus was on bot-driven fraud and logic abuse against public-facing websites and applications, interest jumped, with 81% of respondents citing bot management as a top 10 priority. The most frequently cited concern about bot-attack risks in the next one to two years is account takeover (ATO), which was cited by nearly half of respondents (47%) **(Figure 4)**.

Figure 4.

Most Concerning Types of Bot Attacks

Which of the following types of bot attack(s) is your organization the most concerned about over the next 12 to 24 months?



Note: Multiple responses allowed
Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

Security and Privacy Threat: A Deeper Dive

Bot attacks have caused compliance and legal problems (31%) and a negative impact on data hygiene, governance, or analytics (31%). A combined third of respondents (9% "yes"; 24% "not sure") admitted to the possibility of user credential loss. The majority – 88% – said they are "somewhat concerned" or "very concerned" about the threat.

Top concerns for the next 12 to 24 months, in addition to the threat of site takeover cited by nearly half of respondents, include:

- Site slowdowns caused by overwhelming traffic (37%).
- Sensitive content scraping (30%).
- Credential cracking/brute force attacks (29%).
- Content manipulation via fake or malicious user-generated content (29%).

As 17% of survey respondents reported that bot attacks led to security/IT team restructuring, forward-thinking organizations may want to take stock of the ways bot threats can place a strain on talent resources across the organization, from IT to customer service. As bad bots can steal data, affect site performance, and lead to system breaches, it's increasingly important to consider what this can look like from the customer's point of view.

Online consumers have come to expect an increasingly frictionless experience, especially when making transactions. Businesses ask them to share private information and, in return, consumers expect easy, fast, and secure engagements. If they can't buy inventory or make digital payments in a straightforward manner, they may move on to competitors, and sometimes never come back.

Ironically, some limited yet popular tools that companies use for preventing bot attacks can add a layer of customer dissatisfaction. HUMAN recently completed an independent research study, asking 1,000 consumers about their impressions and frustrations with various styles of CAPTCHA. Only half the respondents reported solving cognitive challenges on the first try. Some 40% of respondents quit a login or transaction attempt because of CAPTCHA frustrations. Nearly two-thirds of respondents were fed up with CAPTCHA.

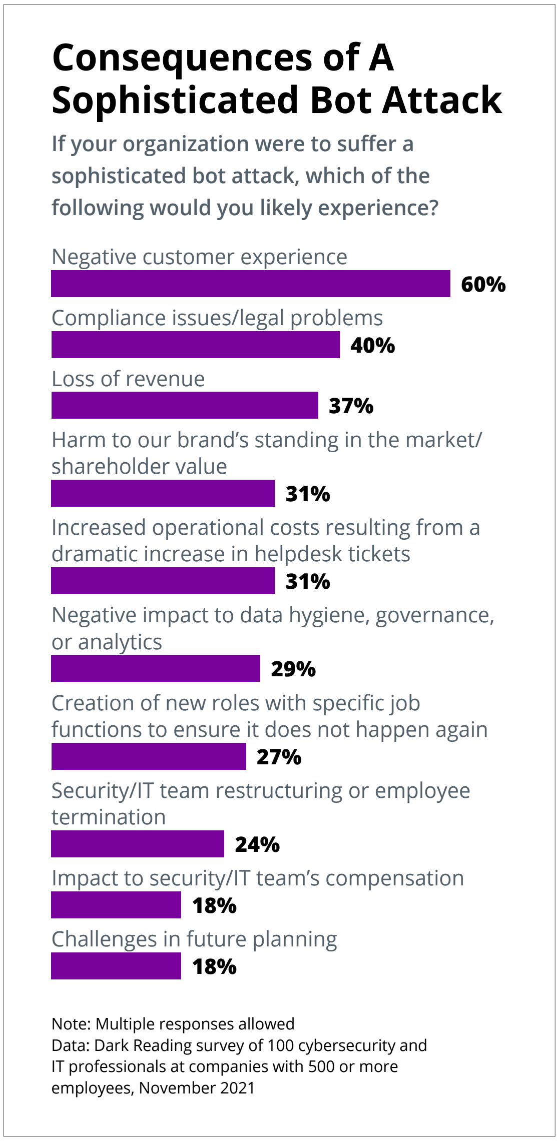
Bracing for Impact

HUMAN wanted to understand how companies are planning to mitigate the rising threats. We asked, "Relative to all of your organization's other security initiatives for the next 12 months, how high of a priority is it to protect public-facing websites and applications from bot-driven fraud and logic abuse (e.g., unwanted automated interaction)?" More than 80% of respondents named bot mitigation as a top 10 priority, and of that group, more than half (53%) identified it as a top five priority. Additionally, 7% of respondents named it as the number one priority for 2022.

The Dark Reading survey asked respondents if their "organization were to suffer a sophisticated bot attack, which would you likely experience?" The answers are distributed across a spectrum of concerns. Among the top three: Negative customer experience (60%), compliance issues/legal problems (40%), and loss of revenue (37%) **(Figure 5)**. Other anticipated consequences:

- Harm to the brand's standing in the market/shareholder value (31%).
- Increased operational costs resulting from a dramatic increase in helpdesk tickets (31%).
- The negative impact to data hygiene, governance, or analytics (29%).
- Creation of new roles with specific job functions to ensure it does not happen again (27%).
- Security/IT team restructuring or employee termination (24%).
- Impact to security/IT team's compensation (18%).
- Challenges in future planning (18%).

Figure 5.



Note: Multiple responses allowed
Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

To get an idea of future preparedness, we set out to understand how companies have engaged their internal teams in managing bot attack threats. Participants were asked to select all the teams their cybersecurity team regularly engaged with in order to address bot-driven fraudulent traffic, engagement, and/or bad data across public-facing websites and applications (and associated infrastructure). Unsurprisingly, IT appears to bear the brunt of management among respondents with 61% reporting engagement. Also, compliance and/or legal was named by 41% and risk management by 38%. It should be noted that 28% of participants involved their customer success/support teams, too.

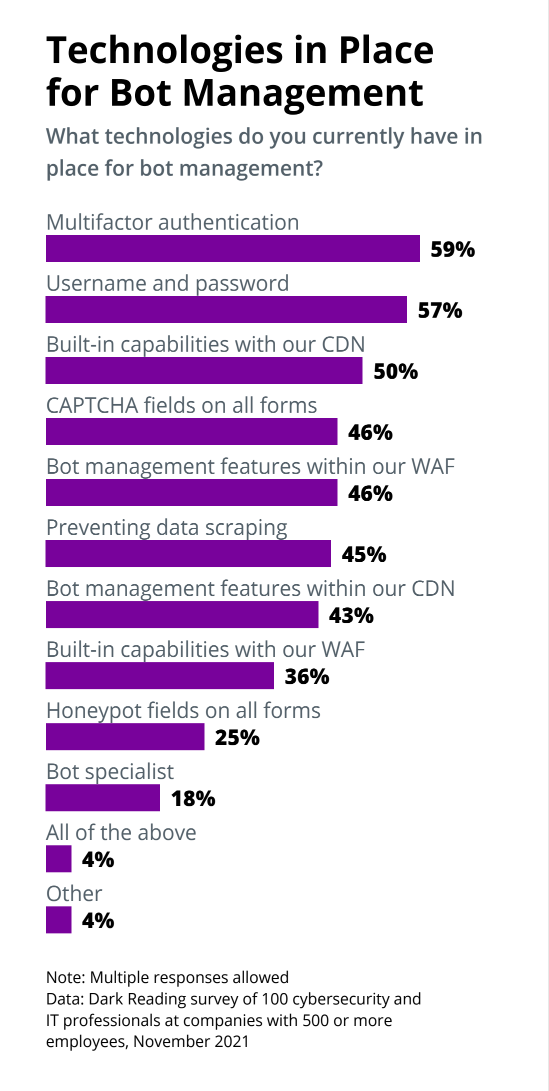
Managing the risk of bot attacks remains a critical aspect of many strategic initiatives within organizations. Results show that 61% of organizations place this goal within cybersecurity, and 47% see it as part of their data governance/compliance initiatives. This demonstrates a continued lack of consensus over ownership of bot mitigation as a security concern. Bot mitigation was also included as a factor in several other strategic areas:

- Cloud migration initiatives (31%).
- Trust and safety (28%).
- Digital transformation projects (26%).
- Digital customer experience optimization (24%).

While three-quarters of respondents said that bot-driven attacks and fraudulent traffic have impacted their organization's digital transformation initiatives, 24% of respondents said they do not currently use bot management tools. A little more than one-third, 35%, indicated they use a bot management feature available in other discrete application security tools (e.g., web application firewall, or WAF). Another third said they use an application security platform that includes bot management capabilities. Only 7% said they use a specialized bot management solution to protect customer-facing applications from fraud and abuse. Among the organizations that employ some form of bot management, the three most popular tactics cited are multi factor-authentication (MFA) (59%), username and password (57%), and the features that are provided by the content delivery network (CDN) **(Figure 6)**.

Most organizations (81%) ranked protecting public-facing websites and applications from bot-driven attacks fraud and logic abuse among their top 10 priorities. However, in practice, just a quarter (24%) used bot management tools and only 7% used a specialized bot management solution.

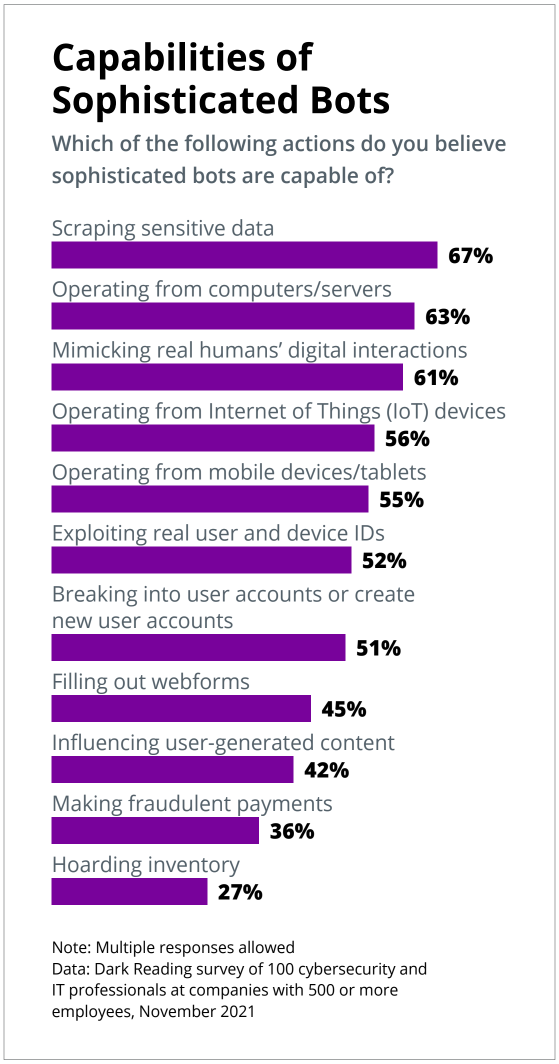
Figure 6.



Understanding the Threat Landscape

Survey findings show that while not all companies prioritize bot management among other cyber threats, there is strong evidence of real organizational impact as well as threat awareness. Nearly three quarters of respondents suspect that a proportion of the traffic on their organization's public-facing websites is generated by sophisticated bots, as opposed to exclusively legitimate human activity. More than a third of respondents estimate non-human traffic to be at least 10%. Further, data revealed that while companies understand the essential capabilities of sophisticated bots, there is room for more education about different types of malicious and fraudulent activities that bots can perform.

Figure 7.



Note: Multiple responses allowed
Data: Dark Reading survey of 100 cybersecurity and IT professionals at companies with 500 or more employees, November 2021

For example, 67% of participants indicated they knew that bots could scrape sensitive data and 61% indicated they knew bots could mimic human interactions **(Figure 7)**.

Concerns also high on the radar of survey participants included the ability of bots to operate from IoT devices (56%) and break into user accounts or create new user accounts (51%), as in the Mirai incident. However, only 27% of respondents said they knew bots could hoard inventory, an attack that could impede sales by preventing real customers from making purchases and damaging the brand experience.

> *Nearly three quarters of respondents suspect that traffic on their organization's public-facing websites is generated by sophisticated bots, as opposed to legitimate human activity.*

Some 80% of respondents agreed or strongly agreed that bots are often controlled by organized and sophisticated cyber criminals; 71% said that most bots are capable of bypassing simple bot protections offered as a feature by vendors. Even so, the majority of organizations are not using bot-specific tools. Just 32% report using the bot management feature available in their application security tools such as the WAF, and 37% report using an application security platform with bot management capabilities. Just 7% report working with a specialized bot management solution.

Overall, data suggests respondents understand the essentials of what's at stake for their organizations in the event of a bot attack. Nonetheless, there is some variation in how respondents perceive their organization's state of readiness or vulnerability. While 45% of participants said their company is susceptible to the different types of bot attacks, just 24% said their companies are prepared to stop these attacks. And 31% believed their organizations would not likely be targeted by these attacks at all.

Do Companies Really Understand the Assignment?

Regardless of where bot management falls on the organization's priority list, results show a significant majority of survey participants recognize the value of addressing this threat. A combined 75% agree or strongly agree that online fraud detection solutions could strengthen current identity and access management (IAM) solutions through analysis of additional risk and identification recognition signals (such as device and behavioral signals analysis). Similarly, a combined 73% agree that adding online fraud detection as part of their current IAM solution could help them remove some of the user friction associated with IAM.

There is a disconnect here, as respondents don't appear to be satisfied with relying on specific features provided as part of broader solutions, as sophisticated bot attacks are bypassing them. As shown earlier, the vast majority don't use specialized bot-management tools, relying instead on broader anti-fraud features such as CAPTCHA and MFA, or capabilities built into the CDN or WAF — measures that are no longer adequate for dealing with increasingly sophisticated bot attacks. Given the potential financial and brand risk, we looked for insights into why many companies aren't prioritizing bot management. For the respondents who said they do not prioritize bot management, their primary reasons were lack of resources (45%), lack of budget (45%), and simply, not thinking it was necessary (45%); multiple answers were allowed.

What would motivate an organization to increase or initiate bot management solutions? Our research indicates that negative customer experience (19%) and harm to the brand's standing in the market/shareholder value (19%) tied as the top factors among survey participants. Compliance issues/legal problems ranked third (18%) in popularity. The results indicate a disconnect between what respondents are concerned about and the actions they will take. Negative customer experience is the top consequence of a bot attack, but respondents are also saying that they won't act on bot management until customer experience is impacted by an attack.

Summary

Thanks to the increased publicity around bot incidents, companies are becoming more aware of the importance of bot risk mitigation. Organizations realize that attacks can draw on resources across IT, security, compliance, and legal teams and, moreover, create negative implications for the customer experience. Nonetheless, companies have a long way to go toward understanding bot mitigation as a specialized form of cyber risk management that requires a dedicated bot specialist that is focused exclusively for the job. This gap can leave organizations vulnerable to a rising, perhaps imminent threat.

About

HUMAN

HUMAN is a cybersecurity company that protects enterprises and Internet platforms from sophisticated bot attacks and fraud to keep digital experiences human. Our modern defense strategy enables Internet-class scale and observability, superior detection techniques, and hacker intelligence and takedowns empowering us to defeat attackers, improving the digital experience for real humans. Today we verify the humanity of more than 15 trillion interactions per week for some of the largest companies and Internet platforms. Protect your digital business with HUMAN.

To **Know Who's Real**, visit www.humansecurity.com.

Survey methodology

Dark Reading conducted an online survey on behalf of HUMAN Security in November 2021 to explore the impact of bot-driven attacks and how large companies are combatting the problem. The final data set used for this report is made up of 100 cybersecurity, engineering, and application security managers at companies with 500 or more employees. Respondents hailed from more than 20 industries primarily from North American organizations.

Some 10% held a CISO job title, and 29% were other C-level, VP-level IT, or cybersecurity managers such as CTO, CDO, or head of risk. Slightly more than one-quarter (26%) of respondents worked at companies of 500 to 999 employees, 26% were from companies with 1,000 to 4,999 employees, and 48% were at companies with 5,000 or more employees.

The survey was conducted online. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa Tech was responsible for all survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.