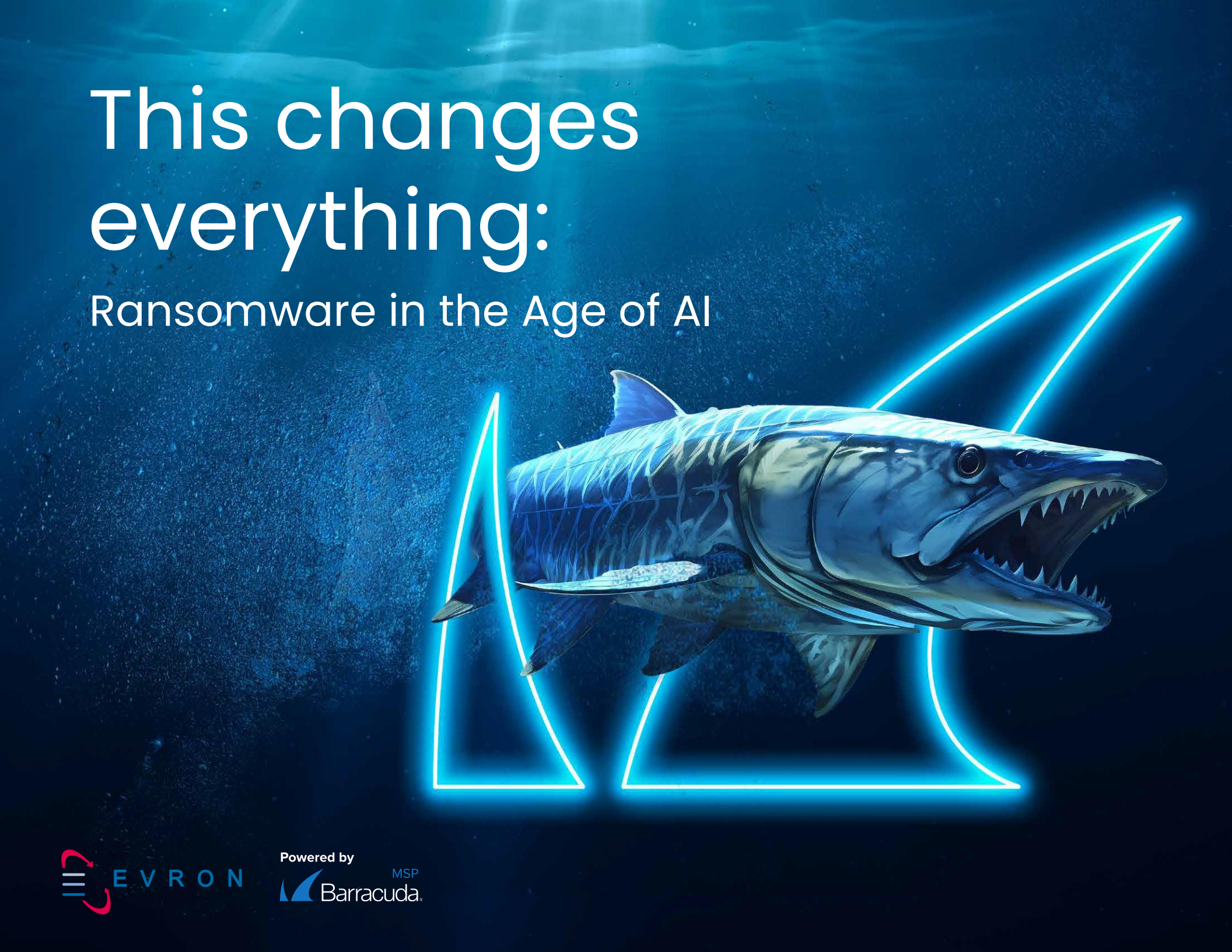
This changes everything:

Ransomware in the Age of AI



EVRON

Powered by Barracuda MSP

The rise of generative AI

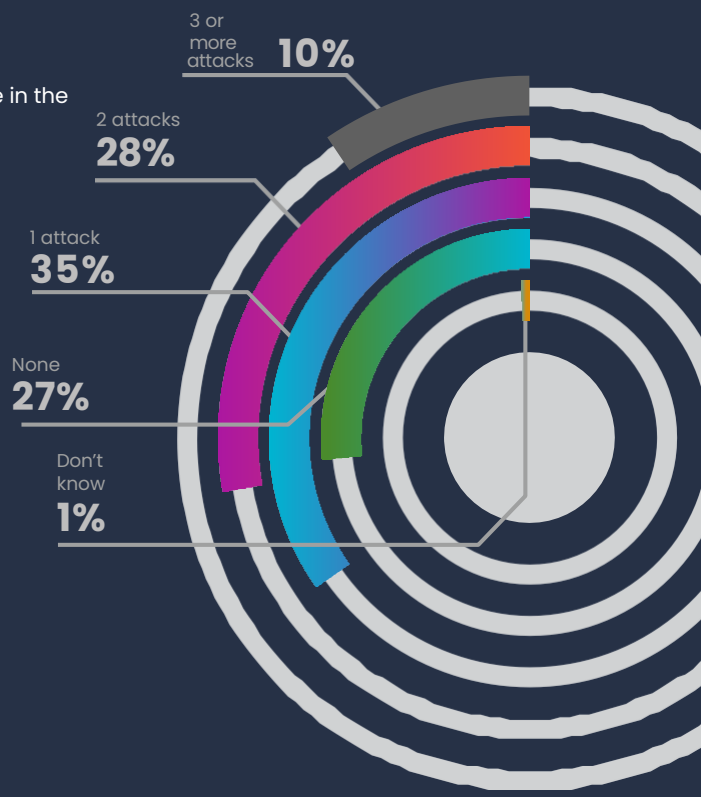
Artificial intelligence (AI) has been hitting the headlines on an almost daily basis in 2023, with developments in generative AI tools (GenAI) such as ChatGPT, Bard, Midjourney, and more being lauded by tech gurus and amateurs alike. Now that GenAI is taking the spotlight, it's vital that we don't forget that while AI can be used for positive activities such as workplace productivity, it can also be deployed for more sinister purposes. Ransomware is one of the areas where bad actors are putting AI to a new and damaging use.

Today's ransomware landscape

These days, ransomware is endemic. Ransomware is malicious software that cybercriminals design and deploy to infect their target's network, take systems down, and encrypt data. Ransomware aims to steal sensitive or confidential information and threaten to leak the data publicly unless a ransom is paid. In 53% of ransomware cases, attackers exfiltrate sensitive data and ask for additional ransom to prevent that valuable data from being publicly exposed. Barriers to entry for ransomware attacks have never been lower, and rewards have never been higher — it's an extremely high-profit, low-risk form of cybercrime that is being committed with increasing sophistication and frequency every year.

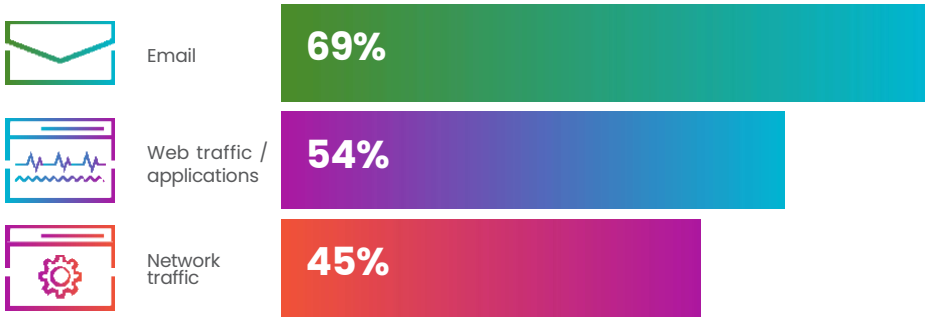
Barracuda's recent market report, 2023 Ransomware Insights, found that almost three-quarters (73%) of respondents were hit with a successful ransomware attack in 2022, and 38% of organizations hit with ransomware in 2022 were repeat victims.

How many successful ransomware attacks did organizations experience in the past 12 months?



Source: 2023 Ransomware Insights

The findings also show that, for 69% of organizations surveyed, some of the ransomware attacks they experienced started with a malicious email. And for larger organizations in the survey — those with over 250 employees — the percentage was even higher, at 75%. These are often phishing attacks, in which an email with a malicious link is disguised as a genuine email from an organization asking for, for example, the compromised individual to enter their log-in credentials to reset a password, or another similar activity.



Source: 2023 Ransomware Insights

Sometimes the link in phishing emails automatically downloads and runs a malicious file, such as a key logger, so that over time they can steal log-in credentials. Credentials are the key to infiltrating the network to further the attack.

In some cases, the initial attacks did not originate from email. Customers who experienced more than one attack were often attacked from multiple vectors. In that same Ransomware Insights report, 54% of the cases reported that they experienced an initial attack through their web applications. In 45% of cases, the successful initial attack was through the organization's network.

In most cases, attackers are using a combination of techniques to exploit any vulnerabilities and get the most value from fully

the attack.

No matter how the attack originates, the end goal is to move laterally across the network in search of exfiltrate data and to lay the groundwork for a ransomware attack. Once the data has been stolen, attackers often try to encrypt or delete backup data to hinder recovery before launching the actual ransomware demand.

AI-powered ransomware

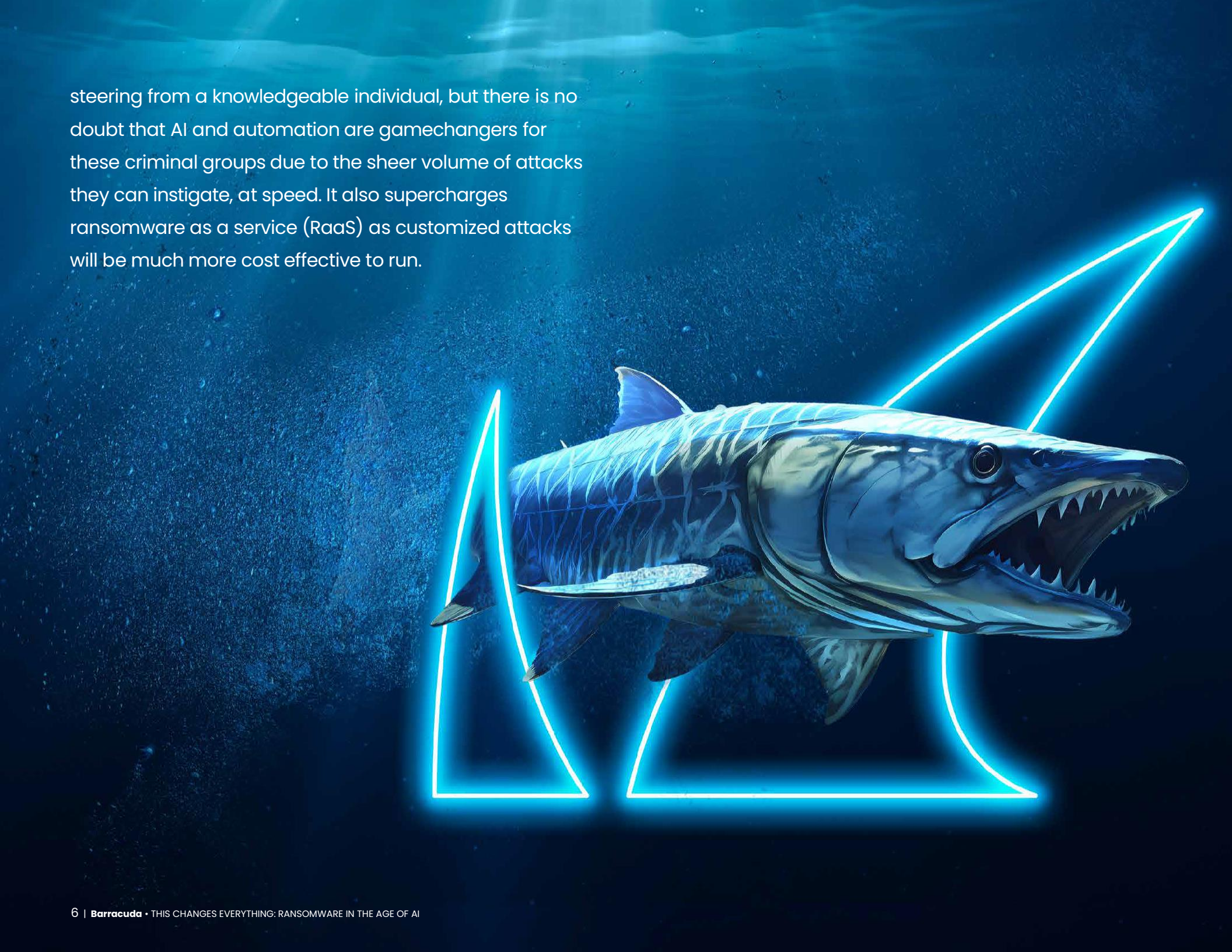
AI-powered ransomware is just what it sounds like: a combination of traditional ransomware and emerging AI technologies. Cybercriminals will employ AI to make their ransomware attacks more effective and to increase the productivity of their organization. We will see AI used in all aspects of ransomware: everything from phishing to negotiating ransom amounts.

AI and automation can be used to craft phishing, vishing (voice phishing over the telephone), and smishing (SMS-based phishing) messages. It can launch network attacks, application attacks, optimize how to hide data exfiltration in normal traffic, as well as research and negotiate ransomware amounts — you name it, AI will be there to optimize it. This is not something to expect in the future. This is already happening now, enabling ransomware attacks to reach new heights, as we've seen in the latest figures from our own ransomware report.

AI-enhanced phishing attacks are perhaps the earliest example of malicious actors putting these new capabilities to use. As soon as a tool like ChatGPT is released, cybercriminals try inventive ways to use it for their own pernicious purposes. Thanks to GenAI chatbots and other natural language processing (NLP) tools, which use large language models (LLMs) to generate text that sounds like it was written by a human, cybercriminals can create messaging for phishing links without the typos, grammatical mistakes, and other tell-tale signs that the email, SMS, or other communication may not be genuine. Non-native speakers can use AI to generate messaging in other languages without worrying that their parlance gives away their false identity. This means that the pool of cybercriminals who can orchestrate convincing attacks has dramatically increased in size, and the phishing, smishing, and vishing messages are much harder to identify as malicious.

Attackers will be better equipped to find and exploit network, application, and other IT vulnerabilities as AI will do much of the work for them using natural language prompts — no advanced coding experience is required. At this point, AI still requires some

steering from a knowledgeable individual, but there is no doubt that AI and automation are gamechangers for these criminal groups due to the sheer volume of attacks they can instigate, at speed. It also supercharges ransomware as a service (RaaS) as customized attacks will be much more cost effective to run.



How to protect against AI-powered ransomware

Barracuda recommends a 1-2-3 protection approach to prepare for and protect your organization against AI-powered ransomware attacks.

The basic steps are as follows:

1. **Protect your email**
2. **Secure your network and applications**
3. **Back up your data**

Protecting your email is a multi-tiered exercise. Organizations must make sure their email security solution also protects credentials, incorporates training that uses AI to identify weaknesses and particularly susceptible individuals and uses a Security Operations Center (SOC) to detect anomalies.
Security Awareness Training (SAT) is essential — your employees must understand how to identify potential phishing attacks and know exactly what to do if they think they've been compromised.

This is not a one-and-done approach: training must be regular and based on current trends in cyberattacks.

Securing your network and applications is also a multi-faceted endeavor and one that we'd need a whole other e-book to cover sufficiently. The basics are: use Zero Trust Network Access (ZTNA) in which you limit who has access to parts of the network and different applications, segment your network, and use your SOC and extended detection response (XDR) to recognize unusual network traffic, protect endpoints, emails, firewalls, servers, and so on. Secure Access Service Edge (SASE) is a great way to ensure that both your cloud and your on-premises architecture are functioning together and protected with the most effective and efficient level of security.

Backing up your data is another crucial element of defending against ransomware. Since ransomware attacks strive to take your systems offline and encrypt your data, organizations must ensure that they have an immutable, secure backup of their data so that they can restore without paying a ransom. This backup should have multiple levels of role-based access controls to ensure that only the necessary individuals can access it. It should also be kept separately from the main network so that if an attack is launched, the ransomware attackers can't find it and encrypt the backup to prevent recovery.

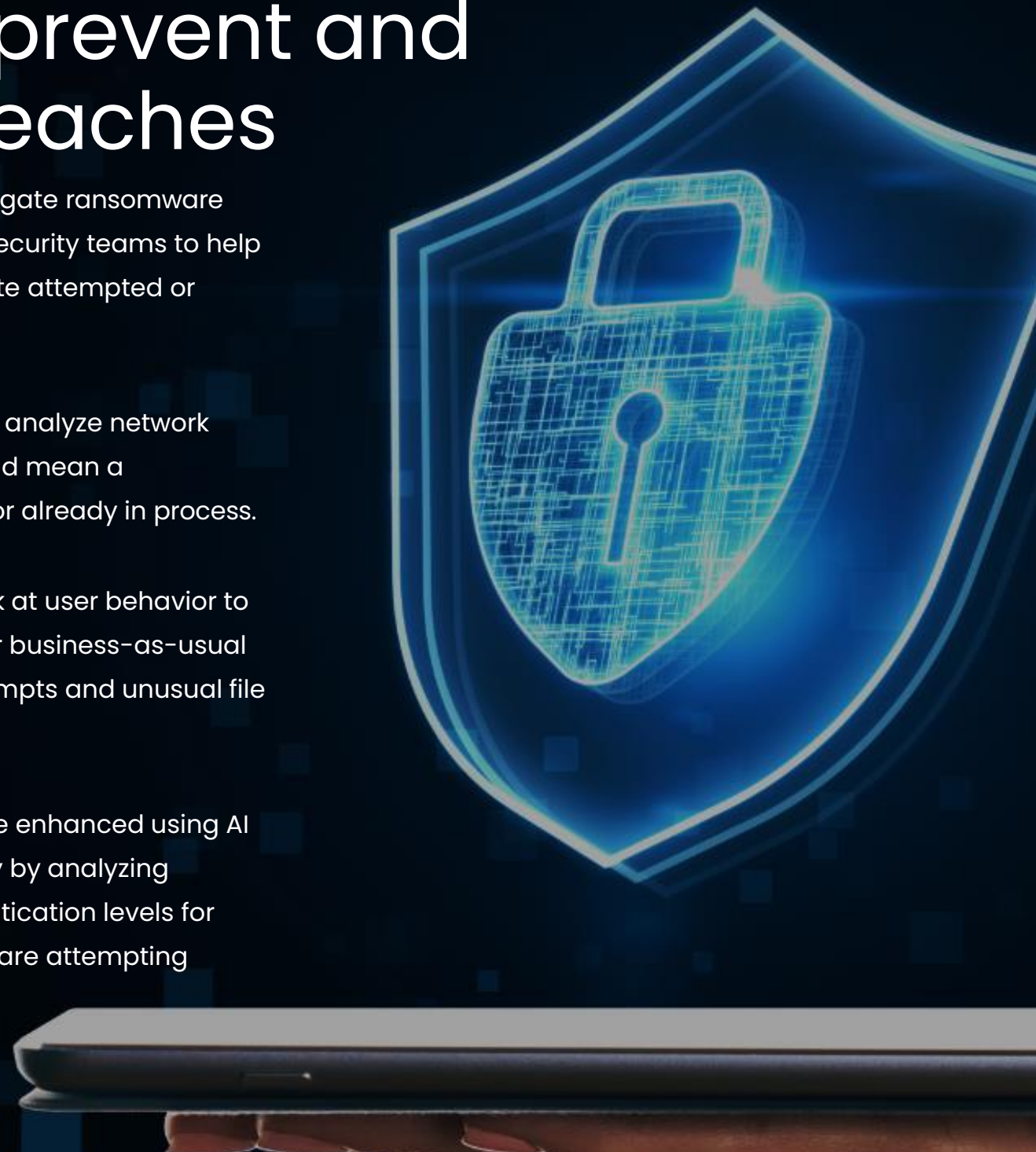
How AI helps prevent and remediate breaches

Just as malicious actors can use AI to instigate ransomware attacks, it can be used by organizations' security teams to help protect them from breaches and remediate attempted or successful attacks:

- AI-enabled ransomware detection can analyze network traffic, file access, and activity that could mean a ransomware attack is either expected or already in process.

- AI-enabled activity monitoring can look at user behavior to identify whether activity is suspicious or business-as-usual — for example, unsuccessful log in attempts and unusual file access.

- Multifactor authentication (MFA) can be enhanced using AI to strengthen an organization's security by analyzing typing speed, requiring multiple authentication levels for sensitive data, and blocking users who are attempting atypical access.



Conclusion

As AI ransomware attacks continue to evolve, so will the AI tools that are developed to protect against and mitigate them. It's important for organizations to stay up to date with all of the cutting- edge technological solutions that help to prevent and remediate these serious, sophisticated breaches. The oft-quoted "fail to prepare, prepare to fail" is pertinent here: it's much more efficient to prepare for and prevent ransomware than to try and remediate a successful attack — and less costly too.

We hope this e-book helps to shine a light on the importance of taking AI-powered ransomware attacks seriously and putting methods in place to prevent them, as well as to leverage the AI tools available to do this.

Barracuda's ransomware solution takes a three-step approach to protecting you from all ransomware attacks, including those powered by AI. We start by protecting your email credentials, then your applications and access, and then protecting your data with a secure backup. For more information or to book a consultation, visit our ransomware solution page.

About Evron

Since 1983, Evron has been committed to helping its clients compete in this world of change. With award-winning SAAS and on-premise ERP applications, they deliver projects that will help businesses become more efficient and profitable.

Evron has been recognized and awarded for their work which has led to them being a Gold Certified Partner with leading companies including Microsoft, Acumatica, Cisco, Barracuda, and more. This gives Evron the ability to fully tailor leading applications to your business needs, as they have for hundreds of other businesses across the continent.