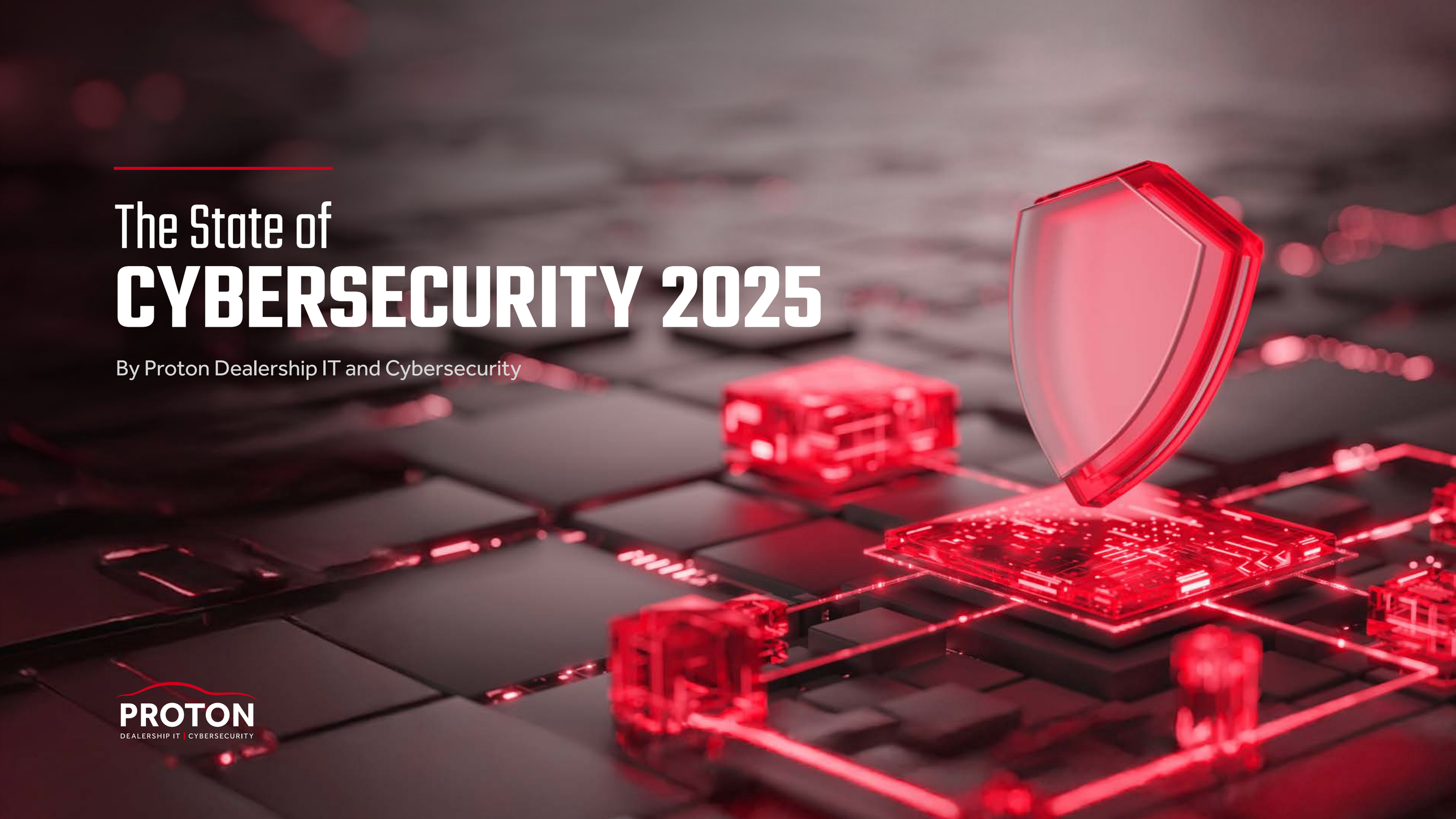
The State of CYBERSECURITY 2025

By Proton Dealership IT and Cybersecurity



PROTON
DEALERSHIP IT | CYBERSECURITY

Introduction

During the summer of 2024, an unprecedented cyberattack on the retail automotive sector left thousands of dealerships unable to perform even basic business functions.

In the days and weeks following that attack, malicious cyber activity rose significantly as dealerships were targeted at much higher rates than immediately prior to the attack. That increased level of threat has persisted to this day.

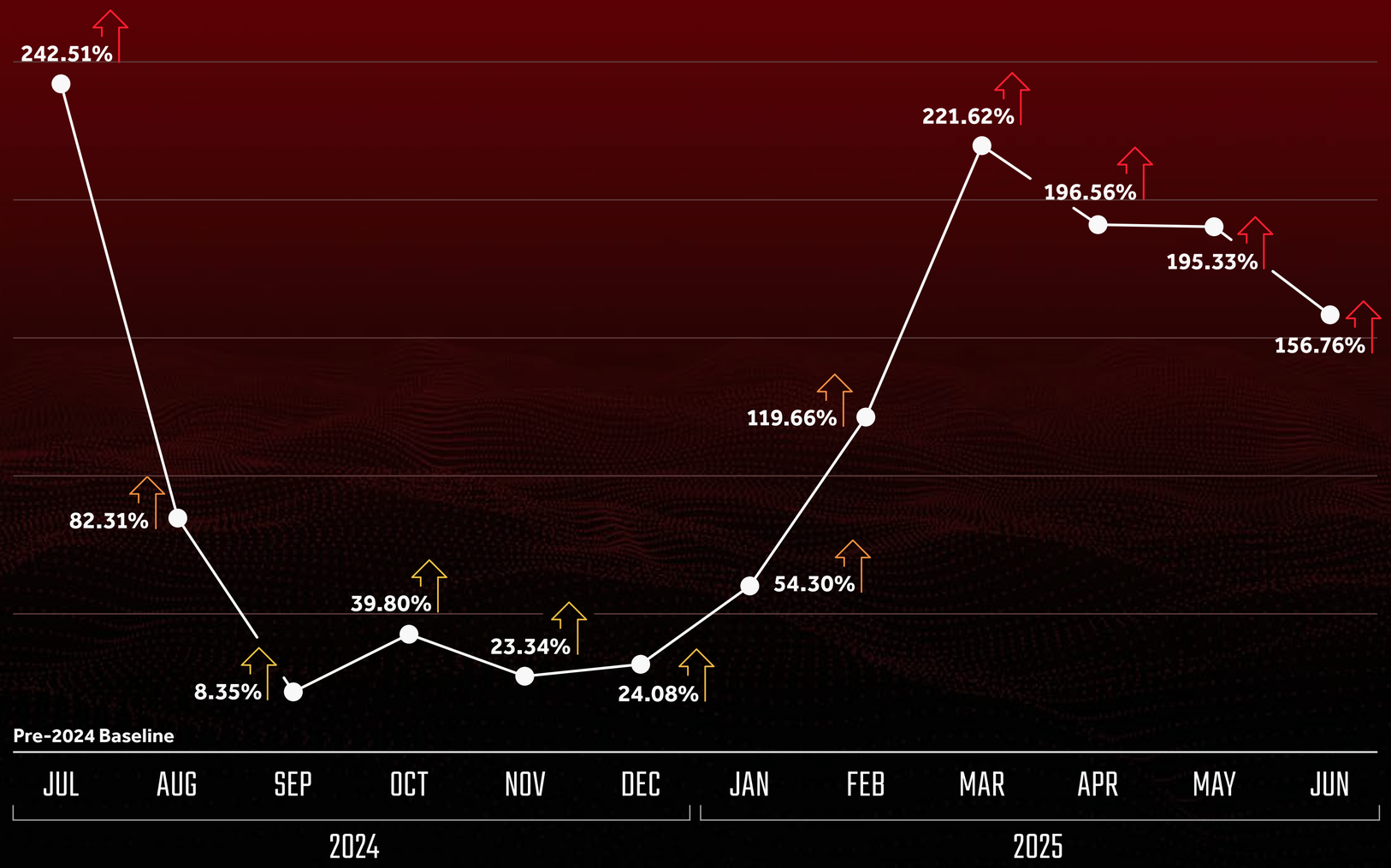
Based on data compiled by Proton Dealership IT and Cybersecurity, this report examines what transpired from July 2024 to June 2025 and identifies trends dealerships need to be aware of so they can take appropriate steps to protect themselves and their investments.

Heightened Activity Persists

According to the data, a spike of attacks followed by steep decline immediately following the incident in June of 2024, set the stage for what followed in 2025.

The instigating event in June highlighted the vulnerability of cybersecurity measures in the retail automotive sector and attack activity has never returned to levels seen prior to June 2024.

As 2024 progressed through the autumn months, the data shows a significant increase in activity. Attackers quickly began to ramp up operations and have maintained a relatively high rate of activity ever since.



MONTH TO MONTH CYBERATTACK TREND

Attacks, Gift-Wrapped for the Holidays

The lag in activity between the inciting incident in June 2024 and the escalation a few months later in December had benefits for attackers and defenders alike. It provided time for some dealerships to bolster their defenses, bringing in firms like Proton to handle cybersecurity.

However, it also allowed dealerships with insufficient or inadequate security to potentially become complacent. Attackers are looking to capitalize on targets like these, as their focus on security wanes. Criminal organizations are notorious for using holidays and off-peak hours to finish their attacks.

Once they have access to a system, they wait to initiate ransomware to help increase the likelihood of financial damage and that the victim will pay out.

The transition from 2024 to 2025 was a prime example of this.

During the month of December, the data shows the start of an escalation in malicious attacks on dealerships, just in time for the holiday season. When it was all said and done, attacks over the holidays were up nearly 110% year-over-year.

Dealerships Are Still in the Crosshairs

Fake CAPTCHA Malware Campaign[1]

In March of 2025, a supply chain cyber-attack was launched that targeted images and videos used by dealership website providers. The attacker successfully injected malicious code into the image files which caused website visitors to unknowingly download and execute malware when attempting to view pictures of vehicles for sale.

Once a user followed the instructions triggered by accessing the images and videos, the malware would access their computer, scraping their web browser history, stealing passwords and controlling the computer remotely.

Ultimately, the attackers could use the remote access and stolen passwords to log into web-based systems and potentially compromise payroll, banking, and OEM systems.

Fortunately, a high quality EDR tool along with expert tuning and 24 hours a day, 7 days a week monitoring can prevent malware like this from turning into a Ransomware event. Proton was the first to identify the malicious content early in the morning of the initial attack. We immediately determined the best way to block and mitigate the attacks and were able to advise the website providers to remove the content.

[1] AutomotiveNews

Conclusion

It's clear the incident in the summer of 2024 triggered an industry wide wake-up call. However, it also exposed vulnerabilities to attackers around the world, who've taken advantage of those opportunities.

While Security Operation Centers scrambled to increase and improve detection strategies, attackers continued to seek new and inventive ways of getting into systems to lock and steal sensitive information.

With malicious activity between roughly 150% and 250% above pre-incident levels, the risk of a cyberattack remains a persistent threat.

Given the current state of Cybersecurity, Proton recommends five things, at a minimum, dealerships need to help protect themselves:

- Train every dealership employee against social engineering and phishing scams.
- Use high quality email filtering and ensure that cloud systems and remote access have Multi-Factor Authentication (MFA) configured for all users.
- Use quality Managed Detection and Response (MDR) programs.
- Rely on professionals to monitor and maintain the dealership's security tools 24 hours a day, 7 days a week.
- Have an incident response and recovery plan ready to go for when the worst-case scenario occurs.

Attacks are targeting dealerships every single day. How well those dealerships are protected makes a difference in whether they will be the victim of a full-fledged ransomware event that shuts them down for several days or weeks, or just a minor 15-minute problem for one user.

For more information about how your dealership can protect itself, visit Protontechs.com

866.605.1027 | INFO@PROTONTECHS.COM | PROTONTECHS.COM