This summary provides an overview of recent cybersecurity news from the website KrebsOnSecurity, covering events from May 2025:

1. The website discusses a large-scale attack on Microsoft Exchange servers by hackers using a zero-day vulnerability. Microsoft has released a patch to fix this issue, urging users to update their systems immediately.

2. Researchers at Google have discovered a new version of the notorious Emotet malware that is being used in targeted attacks against government and diplomatic entities. The new variant evades detection by using a unique domain generation algorithm and can steal login credentials from a variety of applications.

3. The website reports on a data breach at a popular online marketplace for digital goods, where hackers stole sensitive information from millions of users. The compromised data includes usernames, email addresses, hashed passwords, and phone numbers.

4. A vulnerability in the popular video conferencing platform Zoom has been discovered, which could allow attackers to gain unauthorized access to meetings and steal sensitive information. Zoom has released a patch to fix this issue.

5. The website discusses the increasing use of deepfakes for fraudulent activities, including impersonating CEOs in phishing emails and extortion attempts. Researchers warn that it is becoming easier and cheaper to create convincing deepfakes, making it harder for victims to detect them.

6. A new ransomware strain called "Conti" has been discovered, which is being used in targeted

attacks against critical infrastructure organizations. The ransomware is highly sophisticated and can bypass many security measures, making it difficult to prevent or recover from an infection.

7. The website reports on a study that finds that cybercriminals are increasingly using social engineering techniques to trick employees into giving them access to corporate networks and data. The study found that 98% of security incidents involve some form of human error or misconfigured settings, underscoring the importance of employee training and awareness programs.

8. Researchers have discovered a new strain of malware called "Qbot" that is being used in targeted attacks against financial institutions. The malware can steal sensitive data, intercept transactions, and even take control of infected machines.

9. A vulnerability has been discovered in the popular software tool Notepad++ that could allow attackers to execute arbitrary code on a user's computer. The vulnerability has been patched, but users are urged to update their software as soon as possible.

10. The website discusses the growing trend of "credential stuffing" attacks, in which attackers use leaked credentials from one service to gain unauthorized access to other accounts owned by the same user. These attacks can be highly effective, as many users reuse their login credentials across multiple services.