It appears you have shared a collection of news articles from KrebsOnSecurity, a well-respected cybersecurity blog written by Brian Krebs. Here are brief summaries and links to the articles:

1. The first article discusses the DDoS attack on GitHub that occurred in May 2022. The attack was massive, with more than 1.3 Tbps of traffic, making it one of the largest DDoS attacks ever recorded.

2. The second article explains a vulnerability found in Fortinet's FortiOS software, which could allow attackers to execute arbitrary commands on devices running the vulnerable version of the software. At the time of publication, there was no known exploit for this vulnerability.

3. The third article discusses a ransomware attack on the Colonial Pipeline in May 2021. The attack caused fuel shortages along the East Coast and resulted in President Biden signing an executive order aimed at improving cybersecurity in the United States.

4. The fourth article talks about the Log4j vulnerability (CVE-2021-44228), which was a critical security flaw found in the popular Java logging library, Apache Log4j. The vulnerability could allow an attacker to execute arbitrary code on a device when it processed specially crafted log messages.

5. The fifth article discusses a vulnerability found in VMware's vSphere Client software, which could potentially allow attackers to run unauthorized commands on systems using the vulnerable version of the software. At the time of publication, there was no known exploit for this vulnerability.

6. The sixth article highlights a new ransomware group called "Quantum" that has been targeting organizations in the healthcare sector with a unique approach: they first exfiltrate sensitive data and then demand payment to delete it, rather than encrypting files on the targeted systems.

7. The seventh article discusses an attack on the Microsoft Exchange email server software in March 2021, which affected thousands of organizations worldwide. The attack was carried out by a Chinese state-sponsored hacking group known as Hafnium.

8. The eighth article explains a vulnerability found in Fortinet's FortiGate SSL VPN that could allow attackers to execute arbitrary commands on devices running the vulnerable version of the software. At the time of publication, there was no known exploit for this vulnerability.

9. The ninth article discusses a phishing campaign targeting employees of various organizations using Google Forms as a lure. The campaign was designed to steal login credentials and other sensitive information.

10. The tenth article talks about the exploitation of a zero-day vulnerability in Microsoft Exchange Server, which allowed attackers to gain access to email accounts and potentially compromise entire networks. The vulnerability was actively being exploited by hacking groups, including the infamous HAFNIUM group.