The text summarizes several cybersecurity news articles published on the website KrebsOnSecurity. Here's a brief summary of each article:

1. An unidentified hacker group is allegedly planning a large-scale cyber attack on critical infrastructure in the United States, according to a report by CNN. The Department of Homeland Security (DHS) and the FBI are reportedly aware of the threat and working to prevent it.
2. A new malware strain called "Phoenix" has been discovered that steals credentials from compromised devices. Researchers believe the malware is being used in an ongoing phishing campaign against Microsoft Office 365 users.
3. Researchers at FireEye have discovered a hacking group they call UNC2452, which they believe to be tied to the Russian government. The group has been active since at least 2019 and has targeted multiple industries, including defense, energy, technology, and pharmaceuticals.
4. Microsoft has released software updates to fix at least 70 vulnerabilities in Windows and related products, including five zero-day flaws that are already being actively exploited. Two other zero-days also have public proof-of-concept exploits available.
5. The FBI has issued a warning about a new ransomware variant called "Quantum" that is believed to be developed by the same group responsible for the Conti and Hancitor malware. The ransomware uses the RIG Exploit Kit to infect victims, and targets multiple industries including healthcare, education, and government.
6. Researchers at Cybereason have discovered a new espionage campaign targeting political figures in the Middle East using a custom-built phishing tool called "Pelican." The campaign appears to be linked to a group they call APT34, which is believed to be tied to the Iranian government.
7. Researchers at Palo Alto Networks have discovered a new malware strain called "Cobain" that uses a previously unknown exploit for a vulnerability in the Adobe Type Manager Library. The malware has been used in targeted attacks against companies in the Middle East and Africa.
8. A new ransomware variant called "Mystry Ransomware" has been discovered that encrypts data

on compromised devices and then demands payment in Bitcoin. The ransomware uses a combination of techniques to spread, including exploiting vulnerabilities in software and using phishing emails with malicious attachments.

9. Researchers at Volexity have discovered a new malware strain called "Pegasus Spy" that is being used in targeted attacks against human rights activists, journalists, and government officials in the Middle East and North Africa. The malware is believed to be linked to the Israeli surveillance firm NSO Group.

10. Researchers at CrowdStrike have discovered a new malware strain called "Nobelium" that is being used in targeted attacks against government agencies and think tanks in multiple countries, including the United States, Canada, and the United Kingdom. The malware is believed to be linked to a group they call APT29, which is also known as Cozy Bear or the Dukes.