The summary of the articles includes:

1. A group known as "United Russia" is suspected of hacking Russian opposition figures using phishing attacks, malware, and social engineering. The group is linked to the Russian government and is believed to be behind similar attacks in 2016 and 2020.
2. Microsoft has patched five zero-day vulnerabilities in its Windows operating system, including one that is already being exploited by attackers. These vulnerabilities can give attackers elevated privileges on a compromised device.
3. The United States government has extended the deadline for TikTok to sell its U.S. operations to November 12th, giving the Chinese-owned social media app more time to find a buyer. TikTok faces a potential ban in the U.S. due to concerns over data privacy and security.
4. The United States has indicted four Chinese nationals for hacking into American companies to steal trade secrets. The defendants are accused of working on behalf of the Chinese government and stealing intellectual property from at least a dozen U.S. companies in multiple industries.
5. A new variant of ransomware called "Black Kingdom" has been discovered, which encrypts files on infected devices and demands a ransom to unlock them. Black Kingdom is believed to be a spin-off of the Conti ransomware group and uses similar tactics, such as phishing emails and exploiting vulnerabilities in Windows systems.
6. A hacking group known as "APT32" or "OceanLotus" has been linked to attacks on Vietnamese government agencies and companies. The group is believed to be based in Vietnam and is known for using sophisticated tactics, such as spear-phishing emails and zero-day vulnerabilities.
7. Researchers have discovered a new variant of the "Emotet" banking trojan that uses a unique method to evade detection by security software. The new variant uses a legitimate Microsoft service to download additional malicious components, making it difficult for security tools to detect and block.
8. A group of hackers known as "LAPSUS$" has claimed responsibility for breaching the data center

of NVIDIA, a major manufacturer of graphics processing units (GPUs). The hackers allegedly stole source code, internal documents, and other sensitive information from NVIDIA's systems.

9. Researchers have found that attackers are using a new method to bypass two-factor authentication (2FA) on Google accounts. The attack involves tricking victims into downloading malware disguised as a Google authenticator app, which then intercepts 2FA codes and allows the attacker to gain access to the victim's account.

10. A new phishing campaign is targeting employees of Microsoft, Google, and other tech companies with fake job offers. The emails appear to come from legitimate recruiters but contain malicious links or attachments that download malware onto victims' devices.