Threat Landscape

As November dawns, we face the threat actors evolving their tools and techniques by utilizing technological advantages to become more efficient in their campaigns. According to the World Economic Forum, cybercriminals have increased their profits more than the world's third-largest economy after the USA and China[1]. Economic growth allows cybercriminals to invest and recruit more criminals and advance their technology.

In November, the Norwegian Broadcasting Corporation (NRK) were a fraud victim through a spear-phishing attack vector[2]. Criminals bypassed the 2-factor authentication at one of NRK's employees' accounts to hijack the email communication and learnt about the planned transaction between NRK and Icelandic National Broadcasting Service (RUV). Furthermore, they disguised themselves as RUV and changed the bank account number in the invoice. As a result, NRK paid out 80 000 euros to the fraudulent account.

On the 16th of November 2022, Microsoft published an article about the Pass-The-Cookie attack. According to the Microsoft Detection and Response Team (DART), they have observed an increase in token theft by replaying compromised tokens that satisfied the Multifactor Authentication. Hijacking tokens and bypassing multifactor authentication have increased due to the increased usage of private devices in the hybrid world. Unmanaged devices are vulnerable to Pass-The-Cookie attacks where the OAuth 2.0 token is again misused to gain access[3].

Unfortunately, one employee at NRK was a victim of the Pass-The-Cookie attack performed by the fraudulent entity, which compromised the user's account and bypassed multifactor authentication. Microsoft states that Pass-The-Hash attacks can be prevented if devices are managed by Intune in combination with device-based conditional access[3].

Microsoft recommends implementing the following changes to reduce the chance of successful Pass-The-Cookie attacks by:

- Reduce the lifetime of the session.
- Reducing the viable time of a token
- Implement Conditional Access App Control in Microsoft Defender for Cloud Apps
- Reduce risk exposure by disallowing usage of unmanaged devices.

According to the Norwegian National Security Authority (NSM), twelve Norwegian departments have been prone to cyber-attacks since the summer of 2023, performed by advanced adversaries. NSM also stated the consequences of cyber-attacks have become more critical over the last year. These attacks have become more targeted and professionalized[4].

Citrix published two vulnerabilities on October 10, 2023, affecting NetScaler ADC and NetScaler Gateway. According to researchers, CVE-2023-4966 is the most sensitive vulnerability where attackers can read a large volume of memory after the end of a buffer[5].

(1) https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
(2) https://www.nrk.no/norge/nrk-svindlet-for-naer-en-million-kroner-1.16621474
(3) https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/
(4) https://nsm.no/aktuelt/norge-rammes-av-avanserte-malrettede-cyberangrep
(5) https://www.rapid7.com/blog/post/2023/10/25/etr-cve-2023-4966-exploitation-of-citrix-netscaler-information-disclosure-vulnerability/