1、Google doc macadocs (2021)

https://www.techradar.com/pro/google-docs-phishing-scams-are-on-the-rise-heres-what-you-need-to-know

https://www.avanan.com/blog/google-docs-comment-exploit-allows-for-distribution-of-phishing-and-malware

Attack Description: Google doc macadocs is a malware that spreads by disguising itself as a legitimate Google document. Attackers usually trick victims into clicking a link through social engineering techniques, such as phishing emails or instant messages. This link will lead the victim to a seemingly normal Google document page. But in fact, this page is embedded with malicious code or scripts that use the collaborative features of Google documents to spread. Once the victim interacts with the document (such as enabling macros or scripts), the malware will be executed on the victim's computer, which may lead to data theft, system damage, or further malware downloads.

2、Nuclear ransomware (2023)

https://www.malwarebytes.com/blog/threats/nuclear

https://www.resecurity.com/blog/article/ransomware-attacks-against-the-energy-sector-on-the-rise-nuclear-and-oil-gas-are-major-targets-2024

Attack Description: Nuclear ransomware is a type of ransomware that is usually spread through phishing emails, malicious ads, or infected websites. After infection, it scans the victim's computer, finds and encrypts various types of files (such as documents, pictures, databases, etc.). It then displays a ransom note demanding a certain amount of Bitcoin as a ransom in exchange for a decryption key. If the victim does not pay the ransom, the files will remain encrypted and unusable.

3、ZeroAccess (2013)

https://krebsonsecurity.com/2013/12/zeroaccess-botnet-down-but-not-out/

https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/2013/operation_disruption_of_the_zeroaccess_botnet.html

Attack Description: ZeroAccess is a sophisticated Trojan virus that is primarily used to create botnets for click fraud and Bitcoin mining. The attack is usually spread through infected software packages, malicious ads, or compromised websites. After infection, ZeroAccess secretly installs and hides itself on the victim's computer, using rootkit technology to evade detection. It downloads and installs other malicious components that are used to click on ads (generating illegal ad revenue) or mine Bitcoin (using the victim's computing resources to obtain Bitcoin) without the user's knowledge. This malicious behavior not only significantly reduces system performance, but also increases the victim's power consumption.

4、Ponmocup trojan (2013)

https://cfoc.org/trojan-ponmocup-a-detection-and-removal/

Attack description: Ponmocup trojan is a long-term active Trojan virus, mainly used to steal sensitive information of victims. It is usually spread through malicious downloaders, infected websites or phishing emails. Once installed, Ponmocup will record keyboard input, take screenshots and steal information stored in the browser (such as login credentials, banking information, etc.). In addition, it can also install other malware to further compromise the victim's system. The complexity and concealment of Ponmocup make it difficult to detect and remove, posing a serious threat to

users' information security.