1027 Reading

葉富銘 r13922146

1 Topic

Rivers of Phish : Sophisticated Phishing Targets Russia' s Perceived Enemies Around the Globe

2 Summary

This research first report two sophisticated spear phishing campaigns : **Rivers of Phish**, which engage targets with personalized and highly-plausible social engineering in an attempt to gain access to their online accounts, and it is attributed to **COLDRIVER** since the similarity of PDF document structure and metadata, phishing infrastructure and so on. Another is **COLDWASTRE**, which is considered to be the work of separate threat actor due to some differences in PDF and phishing infrastructure, but both of them are considered to be attributed FSB, since the targets they select appears to align with the interests of the Russian government. Then, it explains the reason that government keeps using phishing as a low-cost and efficient technique, gives an overview of the Russian Cyber Espionage Landscape, describe the situation of civil society being targeted by Russia and some other digital threats they may faced. Finally, it gives some recommendations of how to protect yourself.

3 Findings of Research Suitable for NPO

1. **Spear Phishing**
   Executive in NPO may also encounter spear phishing attack. Attackers may forge PDF which pretend the document staff submitted and needs to be signed,

2. **Secure Communication Practices**
   Using multi-factor authentication such as 2FA, security keys and so on, enrolling in programs for high-risk users and adopting five second detective principle can help NPO mitigate the risk of phishing and social engineering attacks.

4 Findings of Research Unsuitable for NPO

1. **Advanced State Resources**
   For most NPOs, the risk from such sophisticated attacks with substantial intelligence capabilities, involving high-level digital espionage tools, like zero-day exploits, is usually lower unless the organization is very large and high-profile.

2. **Physical threats**
   NPO's security issues are often related to financial loss and reputation damage, unless the organization also work in Russia, they are more unlikely face physical violence, such as raids and seizure.

5 Thoughts

In my opinion, phishing perfectly shows that the weakest part of security is people. Despite how powerful the tool and the mechanism is, people may lack the awareness and be easily tricked to leak the private information. The evolution of technique makes phishing even complicated and hard to detect, I think we all need to adopt the five second detective principle : check the sender' s email, check them over a different medium, don' t just click, beware of "encrypted" or "protected" PDFs.