#HITB2021AMS D2T1 - Dissecting Phishing Techniques Of CloudDragon APT - Linda Kuo & Zih-Cing Liao

Published: 2021-06-10 · Archived: 2026-04-05 15:04:13 UTC

North Korea is regarded as the menace to the whole world not only by holding nuclear weapons in reality but bringing damages to cyberspace. For instance, the USD$101 million lost in Bangladesh Bank Heist, or Operation DarkSeoul that paralyzed banks and broadcasters' network systems in 2013. In late 2020, the Cybersecurity & Security Infrastructure Agency of United States (CISA) jointly with Federal Bureau of Investigation (FBI) and Cyber Command Cyber National Mission Force (CNMF) released an alert of a North Korea APT group Kimsuky, implying the significant influence the group has. Learning from the history, we can see how critical the North Korean APTs can affect the world. As one of the most active one in recent years, CloudDragon owns such competence as well. The group's nonstop invasions and mercurial skills shows their strong and plentiful arsenal. Therefore, their victims locate worldwide, including government agencies, think tanks, military, financial service, media, etc. Hence, we are to provide our observation and analysis on the group CloudDragon for better defense and detection. North Korean actors are for their social engineering techniques. Among them, CloudDragon is the cream of the crop. Since many are aware of the importance of infosec, it troubles APT actors a lot. However, it does not seem to bother CloudDragon at all. The group not only applies traditional phishing means but comes up with creative new approach. We collect and categorize them into 3 groups: 1. Prepare the best meals: trending themes 2. Become a fish: phishing sites 3. Build your 'auto fisher': how to bypass 2FA and continuous update of the websites We prepare real cases and in-depth analysis on its various phishing techniques. Some of the personal data collected in previous stage can be reused as baits, followed by CloudDragon;s proprietary backdoor BabyShark and AppleSeed. Thorough technical analysis on the process and malware will be illustrated clearly in the presentation. Windows is not the only platform the group manipulates. We also observed them spreading to android system and manage to approach their targets via different methods. === Linda is currently a Senior Cyber Analyst working for TeamT5. She focuses on Cyber Espionage campaign tracking She devoted herself to cyber intelligence research especially in APT attacks and and Chinese Underground Market. She's also a frequent speaker in international conferences and private seminars, including CODEBLUE, HITCON, FIT, etc. --- Zih-Cing Liao is a Senior Threat Intelligence Researcher from TeamT5. He plays CTF and is interested in reversing, exploit and web security. In TeamT5, he is responsible for improving automated threat hunting and developing tools to accelerate research. He is actively involved in the security community and publishes research at international conferences.
