National Cyber Security Centre
a part of GCHQ

Assessment

NCSC-A/W/1021-22

Business Email Compromise: A growing and evolving threat

Recent figures suggest that Business Email Compromise (BEC) attacks continue to rise. BEC is a digital scam whereby cyber criminals impersonate a victim's trusted work contacts through email spoofing or compromised legitimate email accounts. Their aim is to deceive a victim into making a payment and/or handing over sensitive information.

In the UK, the National Economic Crime Centre (NECC) stated that there were 4600 reported BEC incidents throughout 2021, costing UK individuals and businesses £138 million in losses.

Last month a US Federal Bureau of Investigation (FBI) statement revealed that exposed losses from BEC scams between mid-2016 and December 2021 surpassed $43 billion globally. Between 2019 and 2021, the FBI reported a 65% increase in exposed losses. The FBI's internet crime report highlighted that financial losses from BEC scams in 2021 were 49 times greater than losses recorded from ransomware.

Assessment

BEC attacks remain a core cyber criminal technique, but statistics almost certainly under-represent the true scale of the threat given many incidents go unreported

BEC attacks are a longstanding cyber-enabled criminal threat predominantly emanating out of West Africa. These statistics suggest BEC attacks remain a core cyber criminal technique, but they almost certainly under-represent the true scale of the threat given many incidents go unreported.

BEC tactics, techniques and procedures (TTPs) have become increasingly sophisticated and will highly likely continue to evolve. Cyber criminals are increasingly infiltrating networks, compromising legitimate email accounts and monitoring email correspondence between a victim and their trusted contacts before intervening at an opportune moment. This combination of network access and social engineering appears more authentic than actors simply initiating the communication themselves and is harder to detect.

Despite its prevalence, BEC has been overshadowed by ransomware in both the press and government response. Thus far, BEC and ransomware have largely remained distinct enterprises.

Cyber criminal activity is driven by financial gain, and should ransomware become too problematic or not profitable enough, groups will likely diversify. There is a realistic possibility that ransomware groups will pursue BEC activity in the future. This would likely accelerate BEC's evolutionary trajectory as ransomware operators would almost certainly look to repurpose its more sophisticated tools and infrastructure.

For NCSC guidance on BEC, please see:
https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf