Business email compromise on the rise

Reference: Memo [191001-1] – Version: 1.0
Keywords: cyber-crime, business email compromise, BEC
Sources: Publicly available information

Key Points

- In 2018, Business Email Compromise (BEC) has overtaken ransomware as the main reason behind cyber claims.
- Between June 2016 and July 2019, BEC reportedly accounted for $26,2 billion USD in financial losses worldwide.
- BEC continues to grow with a 100% increase in identified global exposed losses between May 2018 and July 2019.
- Substantial financial losses due to BEC have been publicly reported in August and September 2019.

Summary

On September 10, the US Department of Justice (DoJ) announced[1] the arrest of 281 individuals worldwide for participation in business email compromise (BEC) scams as a result of a months-long operation given the name reWired. Cybercriminals were operating from Nigeria (167), the US (74), Turkey (18), Ghana (15), France, Italy, Japan, Kenya, Malaysia, and the UK. The operation reportedly resulted in the seizure of nearly $3,7 million. According to a statement by the US DoJ, "conspirators stole more than 250.000 identities and filed more than 10.000 fraudulent tax returns, attempting to receive more than $91 million in refunds." In Europe, the Direction Centrale de la Police aux Frontières (PAF) of France, the Squadra Mobile Di Caserta and the Italian National Police, the North Wales Police, the Metropolitan Police Service and the Hertfordshire Constabulary of the UK provided significant assistance.

BEC, also known as "cyber-enabled financial fraud," is a sophisticated scam often targeting employees with access to finances of the company / public organisation they work for. These employees are working with suppliers and/or businesses that regularly perform wire transfer payments. The goal of criminal organisations is to convince them to make wire transfers to bank accounts controlled by the criminals.

According to the AIG insurance company[2], in 2018, BEC has overtaken ransomware and data breach by hackers as the main driver of cyber claims (23% of cyber claims received for BEC against 18% for ransomware). Recent figures released by the FBI indicate that[3], between June 2016 and July 2019, Business Email Compromise/Email Account Compromise (BEC/EAC) accounted for $26,2 billion USD in financial losses worldwide. This threat continues to grow with a 100% increase in identified global exposed losses between May 2018 and July 2019.

Recent cases of BEC related losses include

- In September 2019, the Toyota Group European subsidiary, Toyota Boshoku Corporation announced it was hit by a BEC attack on August 14, that resulted in the loss of 4 billion Yen (~33,9 million Euro).
- In August 2019, the Portland Public Schools district (US) announced it was on track to recover roughly $2,9 million wired by district employees to a BEC scammer, after discovering the fraudulent transactions before the money left the fraudster's accounts.
- In August 2019, a Nigerian national that was on Forbes' list of the most promising entrepreneurs in Africa, was accused of BEC fraud that stole $11 million from one victim alone, Caterpillar industrial and farming equipment (in 2018).
- In August 2019, the Canadian city of Saskatoon was tricked into transferring more than 1 million CAD (~$690.000 Euro) to an actor-controlled account after city employees were compromised in a BEC attack.
- In August 2019, in the US, the Cabarrus County announced it lost $1.728.082,60 USD after being duped by a BEC scam into sending cyber criminals $2,5 million USD.

Comments

EU institutions, bodies and agencies are not immune to this threat. Several of them have been targeted by some form of BEC scams in the past few months. CERT-EU has alerted its constituency about a recent campaign in CITAR-Flash-2019-036. To counter this threat, targeted awareness raising (especially towards employees involved in financial transfers) remains an important asset. CERT-EU reminds its constituency that the organisation of 'phishing exercises' (with the aim of raising user awareness) is part of its service catalogue.

It should also be noted that BEC scams are often conducted together with other forms of fraud, including Romance scams, Employment opportunities scams, Fraudulent online vehicle sales scams, Rental scams, Lottery scams, etc.

[1] https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds
[2] https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf
[3] https://www.ic3.gov/media/2019/190910.aspx