Protecting Personal Investors on UK Investment Platforms from Cyber Threats

Gerard Phillips

Technical Report

RHUL–ISG–2021–2

10 March 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

Investors in the UK are an important part of the country's economy. Collectively they contribute billions of pounds sterling to the financial services sector, which is part of the country's critical national infrastructure.

Increasing numbers of investors use digital platforms and are at increasing risk of cyber-crime. Yet they are largely overlooked and under-represented in cyber security research which focusses principally on threats to financial institutions. This paper goes some way to redress this imbalance.

It examines existing research then develops a new threat model to identify threats to investors. It populates the model with a synthesised dataset of major cyber-attacks on Financial Service Sector (FSS) institutions. Using the new threat model the data is then analysed, threats are identified and new scenarios to defend against those risks are proposed.

Both existing and possible future threats to investors are identified. Around 12% of all existing incidents in the synthesised dataset target investor settings. The motivation for almost all attacks is theft and they are carried out by organised criminal gangs, mostly working from Eastern Europe. They target personal customer accounts and the principal attack vectors are malware, forms of card fraud and "multiple" vector attacks. However, significant gaps in the data suggest this may be only part of a larger picture.

Several scenarios for future attacks on investors are presented. These include high volume and automated attacks on individual investors on their home networks or devices; targeting innovative hybrid card-based applications, such as the Revolut card; and targeting open banking and finance technologies which share personal finance data across different provider platforms.

The research found there were four significant barriers to understanding the threats to investors. First, existing threat models were designed to examine threats to FSS institutions, not investors. Second, UK-specific data was not available. Third, existing models simply do not conceptualise the idea of an "investor threat landscape"; this significantly limits their relevance in understanding threats to investors. Finally, there are almost no threat-centric scenarios for investors and none (yet found) that detail how to prevent and mitigate identified threats.

This paper meets these challenges by innovating a new threat model; creating a synthesised proxy database; proposing new threat landscapes; and developing new strategic and intermediate threat scenarios designed to protect against threats to investors.

In conclusion, recent fraud cyber-crime statistics suggests that investors may already be victims of cyber criminals. An initial survey of investors is conducted which demonstrates investors have only a partial understanding of cyber security. Investment platforms specifically could do more to support investors to learn to be safer online. Finally it is suggested that the national regulator, the Financial Conduct Authority, might share more data on cyber-attacks with the cyber community to protect both investors and companies in the financial services sector.