Authlogics

Strong Authentication Made Simple

The low down on Operation High Roller

How it all went wrong and what to do about it

Whitepaper

Authlogics Ltd, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS LTD MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Introduction

Operation High Roller, as it is now known, is a sophisticated attack on 60+ banks customer accounts via Internet banking which has netted the bad guys between £46 million and £1.6 billon, depending on which article you read.

The exact amount of money stolen isn't all that important to you and I, however how the attack was performed and what can be done to protect against it and other variants is. McAfee has produced a handy report (http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf) about the intricacies and scenarios of how High Roller functions.

Rolling the attack

Operation High Roller relies on malware on a victim's PC which alters the way an Internet banking site of a bank looks and reacts. Its name comes from the way that the malware targets users & businesses with a high bank balance. The Malware obtains legitimate logon and validation details from a user by tricking the user into thinking that they are responding to the banks web site. Once in possession of the details the attacker is then able to use those details to transfer money out of the victim's bank account all while displaying an error, or "please wait" screen to the user. Furthermore, to cover the bad guy's tracks, the malware will also remove evidence of the fraudulent transfers from the Internet banking transaction list and block access to downloadable statements leaving the victim totally unaware of the theft to give the attacker time to move the money around the banking system so it can't be traced or recovered.

Why didn't my key fob save me?

Many banks utilise a 2 Factor Authentication (2FA) system which combines something you know with something you have. Solutions used by banks range from clumsy card reader devices to SMS/TEXT messaging, each with their own merits and pitfalls. These systems aim to prove that you are who you say you are, and not to prove that you are doing what you mean to do.

With the High Roller attack, the bad guy gets around 2FA systems by getting the user to enter the valid 2FA information / One Time Pin (OTP) into their browser. The malware is then able to give this information to the fraudster to use in an attack either directly from the user's machine, or from a remote server – all while showing the user a fake page. Once the fraudster has a valid and unused OTP they can then use it to process their own fraudulent transaction as if they were the legit user.

Turning the tables

While cleaning out the malware is certainly a good start, it's only a matter of time until there is another variant. One needs to look beyond all the fiendishly clever technology and methodology of what makes the High Roller attack successful and focus on the fundamental weakness the attack exploits.

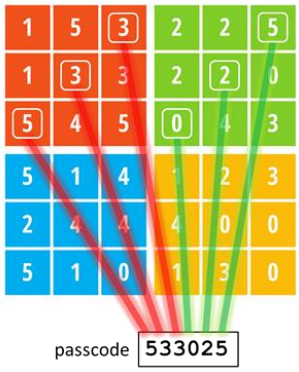
The main weakness is that the actual transaction is not being validated. Instead, the user is being validated at the point of the transaction – two very different things. What is needed is a validation system which can validate the user and the transaction at the same time in a single step. By doing so there is no room for the bad guy to get valid OTP information before the transaction or to change the transaction information after the user has entered a valid OTP code. Furthermore, the user and

transaction elements must be inseparable to the web browser so there is no foothold for malware in the process.

Solving the fundamental problem

Solutions that can simultaneously validate a user and a transaction are not easy to come by, especially at an affordable price for mass deployment. However, one such solution is PINgrid. PINgrid makes use of Matrix Pattern Authentication technology which only requires a user to remember a pattern – a sequence of squares in a grid. The trick to the user validation process is that the pattern is never transmitted during the login process.

PINgrid creates an OTP by placing seemingly random numbers in a matrix and the user identifies their memorized squares by entering the numbers contained in them. The grid is generated and displayed on separate device such as a smart phone or tablet via an app. For standard 2FA, the math behind the numbers in the grid is solely based on time and a hardware value of the smart device – similar to OATH. However, to authorise a transaction additional information is used in the math to generate the numbers in the grid, e.g. an account number, SWIFT code, payee name, transaction amount or a combination of these.



From a user's perspective, at the point of entering payee information on Internet Banking they would also have to enter a transaction code to validate their action. To get the code the user would simply enter the key transaction data, e.g. the account number, onto their phone app which will then present them with a grid of numbers. The user then enters the digits in their memorable squares as their transaction code.

The security in this process lies in the fact that the banks server can make use of the known 2FA hardware ID and the account number when validating the transaction code at the same time. As such, if malware were to modify the transaction information on route to the bank, the transaction code would fail and the bank would not send the money. In addition, any OTP derived without the account number, e.g. during initial logon, would not be able to validate the transaction and again the bank would not send the money.

PINgrid's ability to double check key transaction details via a separate offline smart device gives much needed security and convenience to banks and Internet banking customers.

About Authlogics

Authlogics provides IT security professionals with a fresh alternative to legacy authentication and transaction verification methods. We help companies remove the reliance on password-based authentication and hardware tokens, and encourage the use of self service capabilities. We eliminate costs and administration surrounding card readers and keyring tokens, and innovate without the need to implement expensive biometrics.

Whether you want to authenticate to a Web portal, VPN, firewall, or to a multitude of different Cloud providers, Authlogics offers a range of authentication methods to suit your business. Our solution provides 1.5, 2 and 3 Factor Authentication options, via three authentication technologies (PINpass, PINphrase & PINgrid) and can be delivered via the Web, Mobile App, Email or SMS/TEXT. Additionally, we have several integration agents for various 3rd party systems should you need them.

PINgrid

PINgrid is an award-winning and patented multi-factor authentication and transaction signing solution that is being used in the public and private sector today to transform any mobile device into a soft-token, via a simple offline application, replacing passwords with a memorable pattern that automatically generates a One Time Code (OTC).

PINphrase

PINphrase is a memorable word technology where users are asked for random letters from answers they already know to log in, instead of providing a full password. PINphrase is the only off-the-shelf solution that delivers this type of technology used by many banking web sites.

PINpass

PINpass is a 2 and 3 Factor OATH compliant 6 - 8 digit random code solution. This standard is widely adopted by many vendors and is well trusted. PINpass turns a mobile device into a token via an App or by sending an OTP via SMS or e-mail. Like most OATH solutions, PINpass works with a fixed PIN code which must be remembered, however it can also be used with an AD password or work in PIN-less mode.