FUTURAE

WHITEPAPER

“Fake Support” Attacks

The attack

So-called “Fake Support” attacks target individuals and companies alike. The remote attacker, pretending to call in the name of a financial institution support, or a generic vendor support (e.g., Microsoft), asks the victim to install a remote controlling application (such as TeamViewer, RDS, etc.). The victim is persuaded to follow the instructions from the attacker, as they seem to try to fix computer problems (which are typical) or checking if all is well following an update on the financial institution end. The attacker pretends to want to assist the victim in making sure that they can still access the e-banking portal and perform transactions.

Following the installation of **remote support software**, the attacker observes the victim, and does not interact with the victim’s machine. The victim is instructed to log into the e-banking (performing any necessary secure authentication procedure, such as entering information from a secure token, or similar multi-factor authentication process). Subsequently, the victim is asked to perform a “test” transaction to a new recipient (the so-called money mule, who is colluding with the attacker). The financial service fraud detection system typically prompts the user to perform a step-up authentication (by interacting, again, with the secure token) in order to explicitly confirm the transaction.

Once the “test” transaction is submitted successfully, **the attacker takes control of the victim’s machine through the remote software**, asks the victim to leave the computer on for a few minutes, and **proceeds to perform a number of payments**, typically to the same money mule account.

FAKE SUPPORT PERSONNEL CALLS CUSTOMERS AND ASKS THEM TO INSTALL REMOTE CONTROLLING APPLICATION

The problem

The attack is successful, for a number of reasons:

1. The **fraud detection engine** of the financial service typically works on the following data points: **IP addresses/location, Abnormal user behavior, Unknown recipients whitelisting**

2. Unlike remote phishing attacks, or session hijacking attacks, the following is reported to the fraud engine:

IP address: the usual victim's IP address/location, overall generating from known networks (the IP address is the victim's ISP address, and not the remote attacker's)

Abnormal user behavior: the victim performs standard operations, such as entering a new payment and approving it when the step-up process is initialized, including performing the relevant MFA step

Unknown recipients whitelisting: following the first payment, the money mule account is whitelisted and, no additional steps are required for performing subsequent transactions to the money mule account.

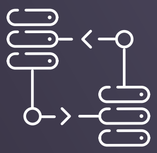
NOTHING SUSPICIOUS DETECTED BY THE FRAUD ENGINE: USER MANUALLY APPROVES TRANSACTION

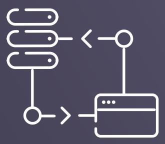
The Solution: Blitz

by FUTURAE

Futurae has developed a **JavaScript component (blitz.js)** that can be installed in the financial services e-banking portal. Blitz will record anonymized user details and activity and submit them to the Futurae processing server. The server constantly feeds on the received information and uses a **trained algorithm to detect if the interaction happening on the e-banking website is local or from a remote actor**. The Futurae server feedbacks to the Blitz component in real time when an attack is detected, and internally logs suspicious activity.

The **feedback loop** can be performed **backend to frontend** (typically used during PoC), or **backend to backend** (typically used for production systems). Furthermore, the solution can also be integrated with existing fraud detection mechanisms already in use by the financial institution.


Backend to Backend


Backend to Frontend

Blitz.js Operations

The blitz.js component needs to be embedded on the e-banking website pages and initialized with a random identifier, that persists throughout a user session. We refer to the technical documentation for a correct initialization and usage.

The JavaScript component will perform the following operations, reporting to the Futurae server:

- On initialization, it will report a **browser fingerprint** (when features are available): user agent, language, color depth, device memory, concurrency capabilities, screen resolution, time zone, storage capabilities, platform, plugins, webGL renderer, AdBlock, touch support, fonts.
- It will hook into the **keypress and mouse movement events** triggered by the user's browser, accumulate them in local storage, and report them in the following form:
    - **'key up', 'key down', 'mouse movement', '<x,y> coordinates', timestamp**
- Upon reporting, the **local storage is cleared**.
- Upon customer request, the Futurae **server does not keep any log** of the browser's IP address.

The Blitz JavaScript operations have been tested on a variety of browsers (Chrome, Firefox, Safari, Opera, Internet Explorer down to IE11). Incompatible browsers would fail gracefully, with no degradation on user's experience (and, clearly, no possibility of attack detection).

COMPATIBLE WITH ALL MAJOR BROWSER

Futurae Server Operations

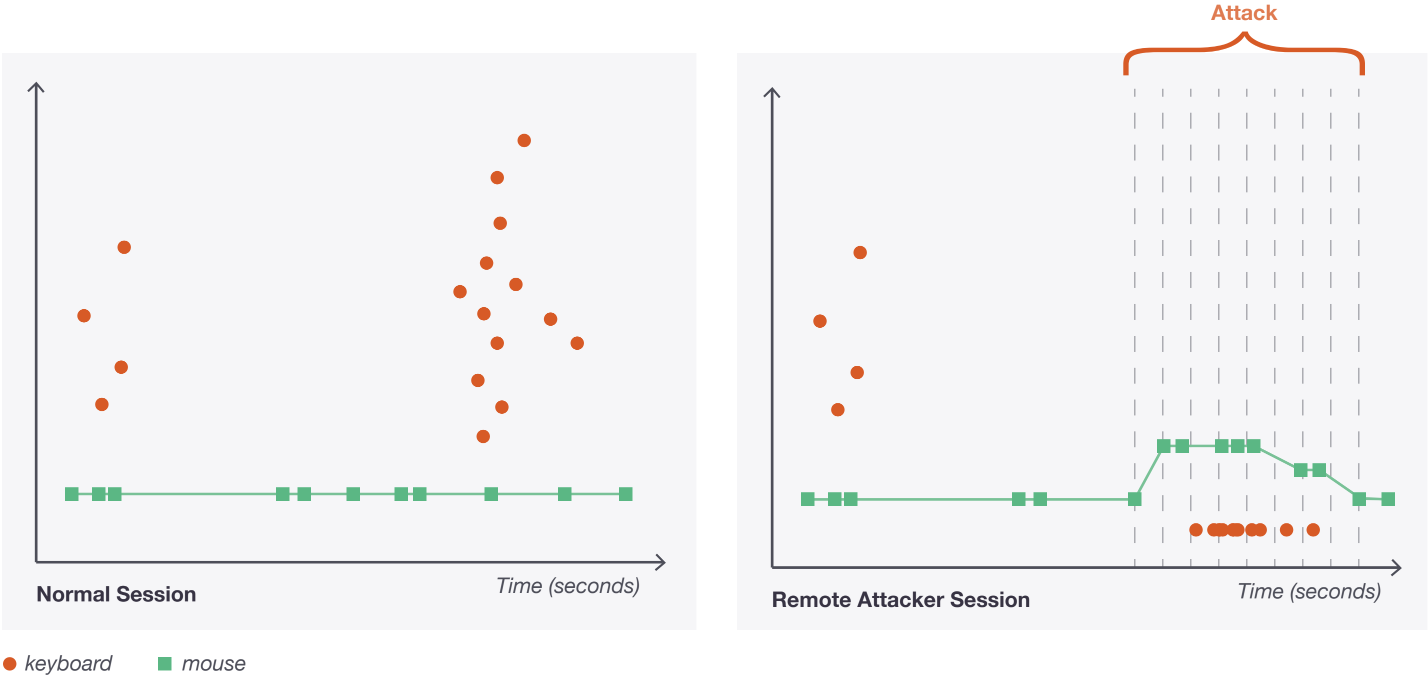
The Futurae Server accepts incoming measurements only when properly authorized by a shared API key. For each session that is created, the server measures a variety of analytics and reports back through the feedback loop channel whether a remote user is interacting with the website.

The Futurae server does not store any sensitive user information or Personally identifiable information and is hosted on a FINMA-compliant Swiss cloud data center.

THE FUTURAE SERVERS ANALYZE IN REAL TIME THE INFORMATION CAPTURED AND DETECT ANOMALIES

Blitz Detection Analysis

A visualization of two user sessions can be seen, as follows. First a legitimate session, second an attack session.



GARTNER COOL VENDOR 2018 - IDENTITY AND ACCESS MANAGEMENT

FUTURAE

- ✓ **Stay Compliant** (PSD2, GDPR, HIPAA, PCI/DSS)
- ✓ **Stay Flexible** (scalable SaaS model that grows with your business)
- ✓ **Stay Secure** (Futurae does not store any sensitive information about your users)

Futurae Technologies AG www.futurae.com sales@futurae.com

swiss made software