NGate: Novel Android malware for unauthorized ATM withdrawals via NFC relay

Lukas Štefanko
Senior Malware Researcher

Jakub Osmani
Penetration Tester

NGate discovery
Technical analysis
Other attack scenarios
Prevention

Digital Security
Progress. Protected.

NGate discovery

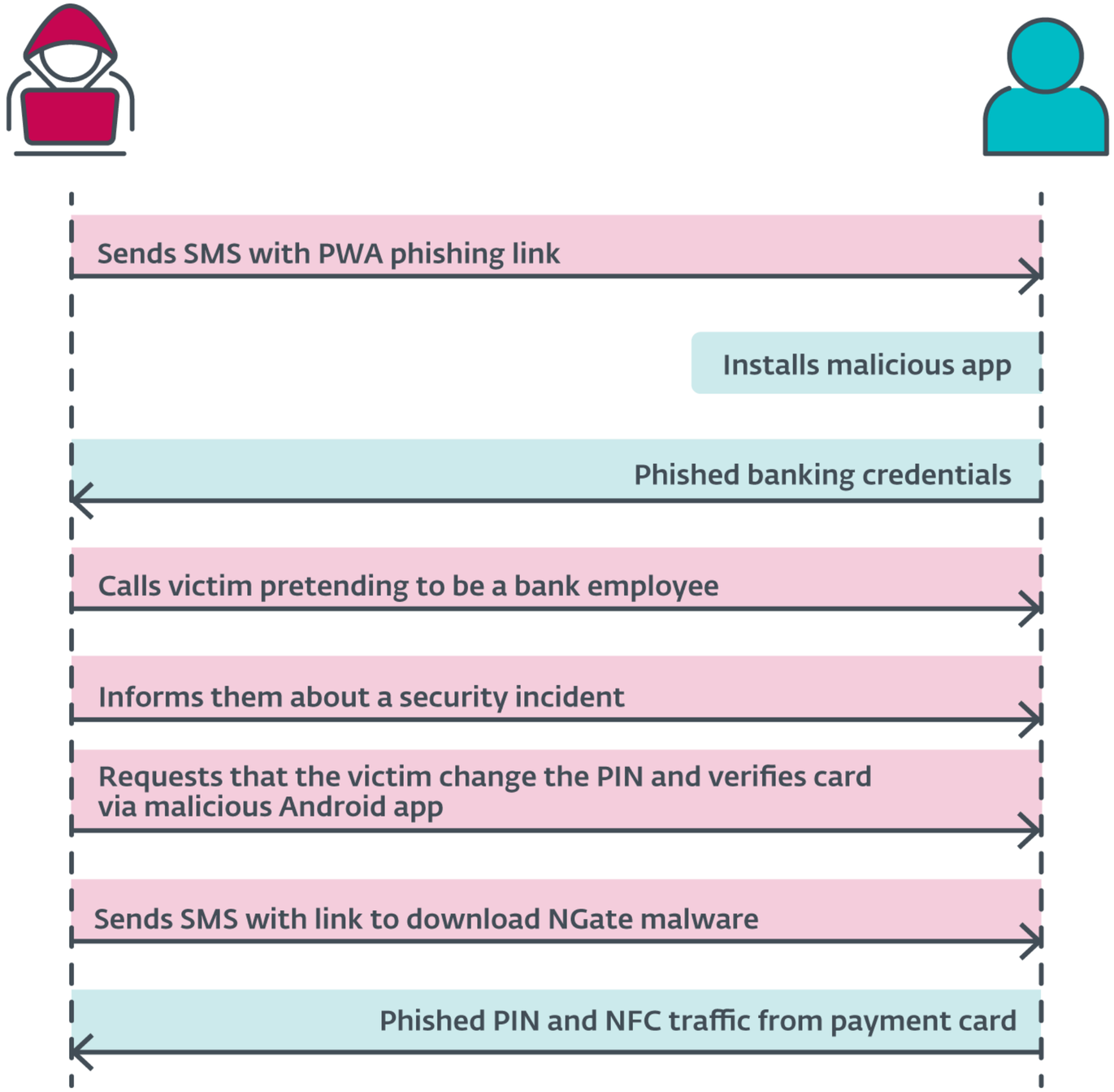
- Arrest in March 2024

NGate discovery

- **Arrest in March 2024**
  - 160,000 Czech korunas (6,000 Euros)
    - The last three victims

NGate discovery

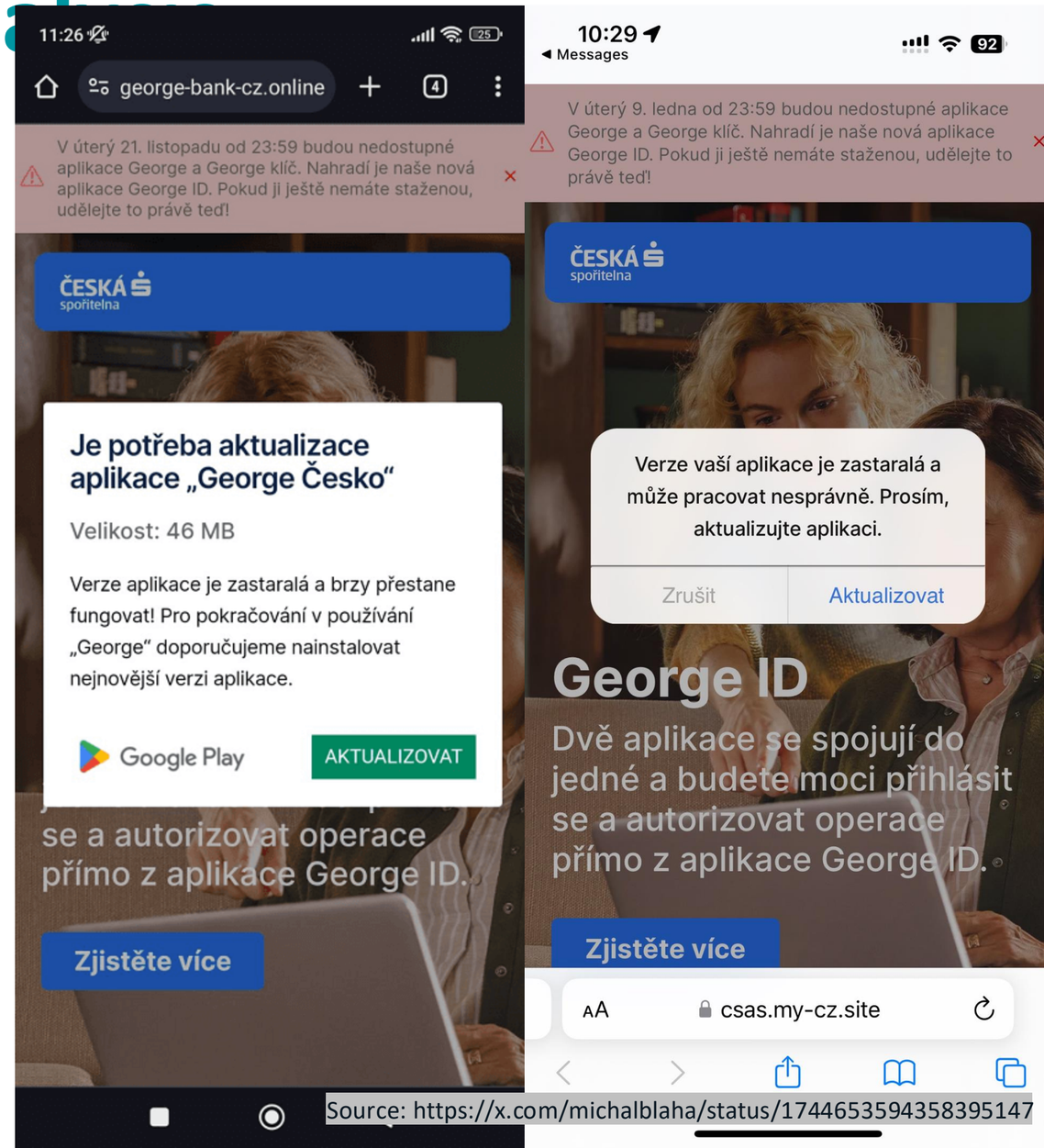
- **Arrest in March 2024**
  - 160,000 Czech korunas (6,000 Euros)
    - The last three victims
- **Discovery**
  - November 2023
- **Distribution**
  - SMS


Sends SMS with PWA phishing link
Installs malicious app
Phished banking credentials
Calls victim pretending to be a bank employee
Informs them about a security incident
Requests that the victim change the PIN and verifies card via malicious Android app
Sends SMS with link to download NGate malware
Phished PIN and NFC traffic from payment card

Technical ana

Attack scenario overview

- Malicious Progressive Web Apps
  - Android, iOS
- Malicious WebAPK
  - Android
- NGate



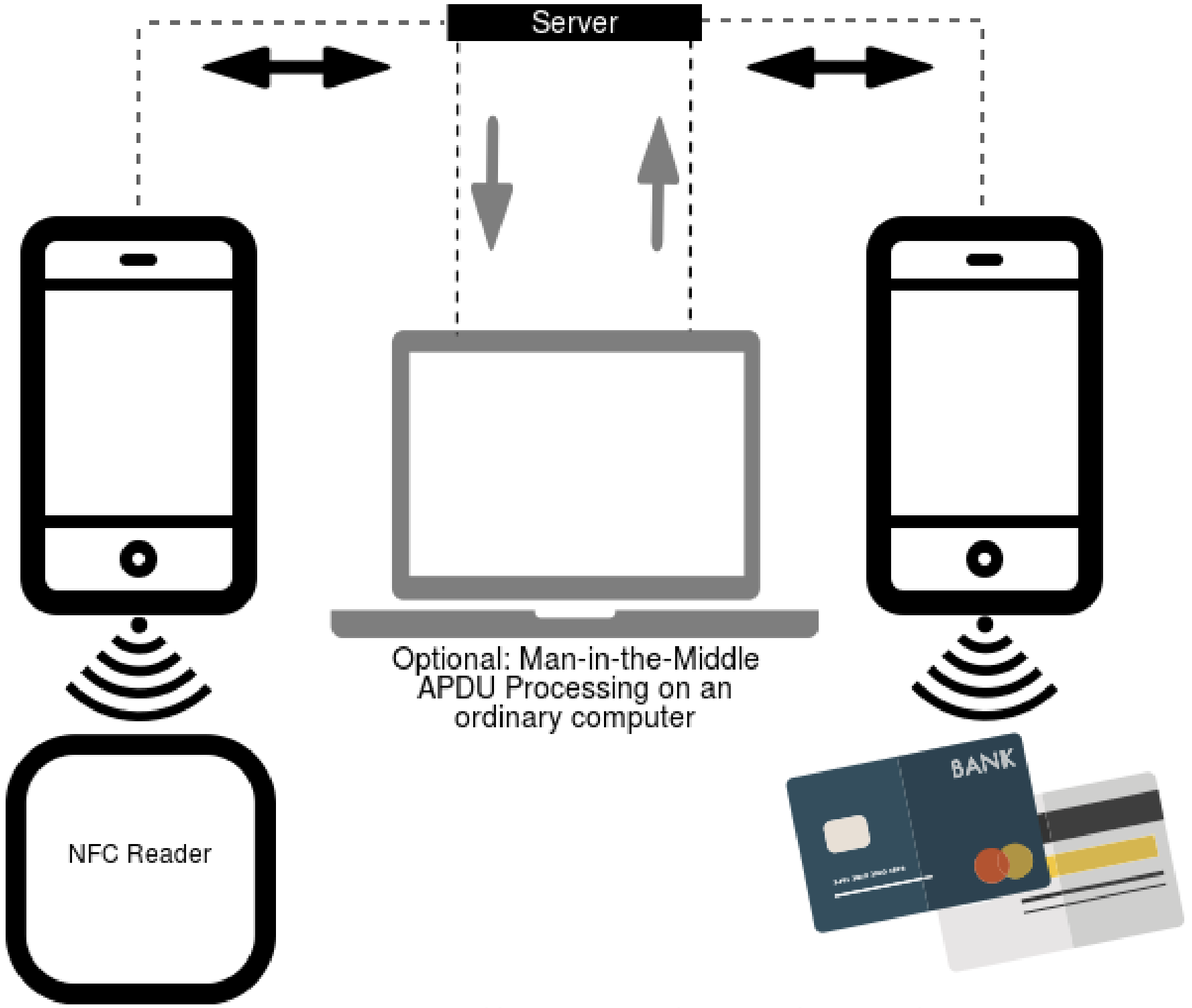
Source: https://x.com/michalblaha/status/1744653594358395147

Technical analysis

```
@JavascriptInterface
public void setMode(final String tokenM, String mode, int session, int port, String host) {
    BaseNetworkFragment.this.token = tokenM;
    BaseNetworkFragment.this.token = Settings.Secure.getString(BaseNetworkFragment.this.getContext().getContentResolver(), "android_id");
    SharedPreferences prefs = PreferenceManagerFix.getDefaultSharedPreferences(BaseNetworkFragment.this.getActivity());
    prefs.edit().putString("session", String.valueOf(session)).putString("port", String.valueOf(port)).putString("host", host).apply();
    if (mode.equals("reader")) {
        BaseNetworkFragment.this.onSelect(true);
    } else if (mode.equals("tag")) {
        BaseNetworkFragment.this.onSelect(false);
    } else {
        BaseNetworkFragment.this.reset();
    }
    new Handler(Looper.getMainLooper()).post(new Runnable() { // from class: de.tu_darmstadt.seemoo.nfcgate.gui.fragment.BaseNetworkFragmen
        @Override // java.lang.Runnable
        public void run() {
            try {
                JSONObject jsonObject = new JSONObject();
                jsonObject.put("token", tokenM);
                jsonObject.put(NotificationCompat.CATEGORY_EVENT, "setMode");
                String jsonString = jsonObject.toString();
                BaseNetworkFragment.this.webview.loadUrl("javascript:eventResponse('" + BaseNetworkFragment.this.token + "','setMode')");
                Log.d("uerbrt", jsonString);
            } catch (JSONException e) {
                throw new RuntimeException(e);
            }
        }
    });
}
```

Technical analysis

- **NGate**
  - Phishing
    - Account info, PIN
    - C&C
      - JavaScript interface
  - NFCGate tool
    - Secure Mobile Networking Lab at the Technical University of Darmstadt in Germany
    - Capture, relay, replay, clone
  - Video demo



Source: https://github.com/nfcgate/nfcgate/wiki

Other attack scenarios

- **NFC tags**
  - UID Mifare
- **Contactless payments**
  - limited

Prevention

- Official app stores
- RFID blocker
- Mobile wallet apps

Questions?

Digital Security
Progress. Protected.

Thank you.