FINAL PROJECT

SOFTWARE SECURITY

Threat Mapping & Analysis

"Dana Easy - Uang Pundi" Mobile Application

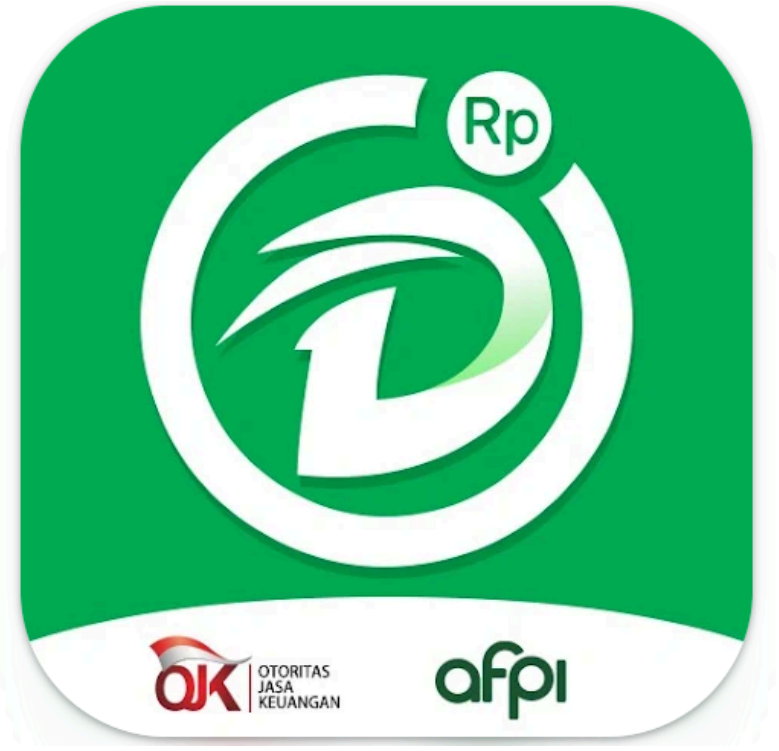
Group 7:

- Dinanti Nabilah Ardelia (2702313615)
- Jovan Rivaldo (2702303500)
- Michelle Aurelia Anggriawan (2702247645)
- Rachelle Celina Salim (2702326800)

JUNE 2025

TABLE OF CONTENTS

Background Apps



*Gambar Aplikasi **Dana Easy - Uang Pundi***

Dana Easy - Uang Pundi merupakan aplikasi *fintech peer to peer lending* atau biasa yang disebut pinjaman online (Pinjol). Apps ini merupakan sebuah lembaga penyedia jasa yang memberikan pinjaman berupa dana (Uang) tanpa terjadinya pertemuan langsung dengan cara mengumpulkan beberapa dokumen dan data diri lalu menunggu hasil konfirmasi dari pencairan ataupun pengiriman dana. Lebih gampang, mudah, dan tidak banyak langkah yang dilakukan serta bisa diakses dimana saja.

Fitur Aplikasi

Sama seperti aplikasi pinjol pada umumnya fitur yang ada di apps ini juga tidak kalah simpel yaitu pendaftaran, peminjaman, pembayaran, dan tab-tab yang sering ada di sebuah aplikasi seperti profile,home,dll.

Analisis Fitur

Menurut kami fitur pendaftaran pada apps ini yang menjadi pintu utama terhadap ancaman yang ada dalam aplikasi ini. *Flow* dari fitur pendaftaran ini sangat mudah tanpa keabsahan yang jelas;

Pertama pengguna akan mendownload aplikasi dari playstore, banyak orang yang beranggapan "*Aplikasi ini kan udah ada di playstore terpercaya dong pastinya?*", sebenarnya hal ini tidak bisa menjadi acuan apakah aplikasi aman digunakan.

Kedua sebelum membuka aplikasi pengguna dimintai akses Kontak, Galeri, Penyimpanan, Pesan & Telepon yang sebenarnya hal diatas ini tidak ada hubungannya terhadap Pinjaman yang akan kita lakukan.

Ketiga pengguna akan mendaftar dan dimintai verifikasi yang sangat simpel yakni Foto KTP dan juga Foto Selfie. Sangat simpel sehingga banyak yang akan memakai apps ini tanpa tau keamanannya ("*Yang penting mahh sat sett*")

Analisa kami mengenai flow dari fitur ini yang pertama sangking sangat simpelnya pasti banyak orang yang akan tertarik dan terjadinya persebaran informasi *mouth to mouth* yang dilakukan, Apps ini sukses untuk memberi kesan "*sangat mudah dipakai*" berkat flow yang tidak ribet dan tidak memakan waktu yang banyak. Dari segi apps sendiri dengan mereka meminta akses yang tidak seharusnya seperti Kontak dan Galeri dari sini kami mulai curiga dan pasti akan menimbulkan ancaman seperti pencurian kontak pengguna, pencurian data pribadi, penyalahgunaan data pribadi, sampai tindakan yang melanggar hukum lainnya.

Flow peminjaman yang hanya melampirkan KTP dan Selfie tanpa membutuhkan kredensial lainnya juga menjadi ancaman yang sangat krusial dimana bisa saja pengguna melampirkan KTP orang lain dan selfie orang lain sehingga orang lain akan berdampak padahal tidak melakukan apa-apa.

Scenario Threat

Berikut beberapa scenario yang kelompok kami pikirkan:

- **Kepercayaan Pengguna**: Dikarenakan Apps ini sudah ada di playstore beberapa pengguna akan mencoba apps ini tanpa pikir konsekuensi yang akan didapatnya. Di gambar logo dari Apps ini sudah ada OJK-nya namun sebenarnya aplikasi ini belum mendapatkan legalitas dari OJK yang membuat sebenarnya aplikasi ini pinjol illegal.

- **Izin Akses Mencurigakan**: Aplikasi ini meminta akses yang mungkin seharusnya tidak diperlukan seperti Kontak, Galeri, Pesan, dll. mungkin kalau kamera masih bisa dipahami dikarenakan butuh untuk selfie dan foto KTP namun kontak?, galeri? untuk apa?? ini bisa menjadi sebuah ancaman dimana terjadinya pencurian data pribadi, penyalahgunaan data, dll. Kami memikirkan sebuah skenario dimana jika pengguna melakukan pinjaman dan tidak membayar sesuai tenggat yang diberikan makan developer bisa mengancam menggunakan data yang sudah didapat dari akses yang dimintai aplikasi seperti kontak dan galeri. Developer bisa mengancam dan menyebarkan serta meneror semua kontak yang terhubung dengan pengguna, membuat propaganda dari data yang didapat, mengancam menyebarkan rahasia/privacy dari pengguna.

- **Pinjaman Mudah**: Dengan melampirkan KTP dan selfie pengguna sudah bisa mendapatkan pinjaman dengan begitu mudahnya tanpa adanya verifikasi kredensial lainnya, memang simpel dan mudah tapi mematikan bayangkan saja jika kalian mendapatkan 10 data ktp dan selfie orang, dengan menggunakan data itu kalian bisa melakukan pinjaman menggunakan data orang lain dan mendapatkan uang ditambah jaman sekarang makin maraknya kebocoran data penduduk serta AI yang berkembang seiring berjalan waktu menggunakan Deepfake.

STRIDE ANALYSIS

S - Spoofing

- **Meniru Aplikasi Legal:** Mereka menggunakan nama-nama generik seperti "Dana Easy", atau bahkan meniru nama dan logo pinjol legal yang terdaftar di OJK untuk mengelabui korban agar percaya bahwa mereka adalah layanan keuangan yang sah pada gambar logo dari Apps ini sudah ada logo OJK-nya namun sebenarnya aplikasi ini belum resmi izin OJK.
- **Meniru Pihak Berwenang:** Saat proses penagihan, *debt collector* mereka sering kali meniru identitas aparat hukum (polisi, pengacara) atau utusan dari OJK. Mereka mengirim pesan dengan ancaman palsu akan "memproses hukum" atau "memenjarakan" korban untuk menimbulkan kepanikan.

T - Tampering

- **Memanipulasi Foto Korban:** Ini adalah bentuk *tampering* yang paling terkenal. Pelaku mengunduh foto dari galeri HP korban (yang izinnya sudah mereka dapatkan secara paksa), lalu mengubahnya (tampering) menjadi gambar asusila atau meme yang memalukan. Gambar hasil manipulasi ini kemudian digunakan sebagai alat pemerasan.
- **Mengubah Detail Pinjaman:** Pelaku dapat secara sepihak mengubah detail pinjaman di sistem mereka (misalnya, menambah denda fiktif) tanpa sepengetahuan korban. Karena tidak ada layanan pelanggan yang transparan, korban tidak memiliki cara untuk membantah.

R - Repudiation

- **Menyangkal Pembayaran:** Korban bisa saja sudah membayar lunas, namun pelaku menyangkal telah menerima pembayaran tersebut dan terus melakukan penagihan. Korban sulit membuktikannya karena tidak ada bukti pembayaran yang sah dan diakui.
- **Menyangkal Aksi :** Perusahaan pinjol ilegal akan selalu menyangkal bahwa mereka bertanggung jawab atas teror yang dilakukan *debt collector*. Mereka akan berkilah bahwa itu adalah "oknum" yang beraksi di luar kendali mereka, padahal itu adalah prosedur operasi standar mereka.

I - Information Disclosure

- **Pemanenan Data Pribadi:** Sejak awal, aplikasi ini meminta izin akses ke seluruh kontak, galeri, SMS, dan file di HP korban. Ini adalah tindakan pengungkapan informasi yang disengaja oleh korban karena ditipu.
- **"Sebar Data" sebagai Senjata:** Ancaman terbesar adalah pengungkapan informasi secara sengaja dan masif. Pelaku akan menyebarkan data pribadi korban (nama, foto KTP, jumlah utang) ke seluruh daftar kontak HP korban.

Mereka secara sengaja melanggar privasi untuk mempermalukan, mengisolasi, dan menekan korban agar membayar.
- **Risiko Kebocoran Data Massal:** Server tempat pinjol ilegal menyimpan data korban (KTP, NIK, daftar kontak) kemungkinan besar tidak aman. Hal ini membuka ancaman pengungkapan informasi lebih lanjut jika server mereka diretas, membocorkan data ribuan korban sekaligus.

D - Denial of Service

- **Memblokir Akses Pembayaran:** Pelaku dapat dengan sengaja membuat sistem pembayaran mereka "error" atau memblokir akun korban menjelang jatuh tempo. Hal ini membuat korban tidak bisa membayar tepat waktu. Akibatnya, korban dianggap telat dan bisa langsung dikenakan denda besar serta menjadi target penagihan kasar.

E - Elevation of Privilege

- **Aplikasi sebagai Alat Peningkatan Hak Akses:** Dengan menyamar sebagai aplikasi pinjaman, pelaku berhasil menipu korban untuk memberikan hak akses setingkat administrator terhadap data paling pribadi di ponsel mereka (kontak dan galeri). Aplikasi ini "meningkatkan hak aksesnya" dari sekadar aplikasi finansial menjadi alat mata-mata (*spyware*).
- **Potensi Malware Tambahan:** Aplikasi ilegal ini bisa saja mengandung kode berbahaya lain (*malware*) yang bertujuan untuk mendapatkan kontrol lebih dalam terhadap perangkat korban, seperti mencuri kata sandi atau memata-matai aktivitas perbankan.

Conclusion

Setelah kita bedah semuanya, jelas sekali ada dua dunia yang berbeda, pinjol resmi OJK yang merupakan alat keuangan, dan pinjol ilegal yang pada dasarnya adalah jebakan kriminal berkedok aplikasi. Analisis tadi membuktikan kalau aplikasi ilegal itu bukan sekadar "tidak aman", tapi memang sengaja dirancang untuk jadi jahat. Fitur-fitur mengerikan seperti kemampuan menyebar data kontak, mengancam, hingga mengambil foto kita untuk meneror, bukanlah sebuah kesalahan sistem, melainkan memang itulah cara kerja mereka sejak awal.

Iming-iming dana cair cepat itu hanyalah umpan di depan. Begitu data pribadimu terutama isi kontak dan galeri foto kita sudah mereka sedot, aplikasi itu berubah menjadi senjata yang siap menghancurkan diri kita. Masalahnya bukan lagi sekadar soal utang yang bunganya mencekik, tapi masalah hidup yang diobrak-abrik. Mereka tidak akan segan meneror seluruh teman dan keluargamu, menyebar fitnah, dan melakukan pelecehan brutal hanya karena kamu telat membayar.

Jadi, solusinya cuma satu, bangun pertahanan diri yang kuat. Mitigasi terbaik adalah pencegahan. Pertama, jangan pernah malas untuk mengecek legalitas pinjol di situs resmi OJK sebelum mengunduh apapun. Kedua, dan ini yang paling penting, perhatikan izin akses aplikasi saat proses instalasi. Jika sebuah aplikasi pinjaman meminta akses ke Kontak atau Galeri Foto, anggap itu sebagai tombol alarm bahaya. Langsung tolak dan hapus aplikasi itu tanpa pikir panjang.

SOURCE

Abdullah, A. (2021). Analisis Pengetahuan Pinjaman Online Pada Masyarakat Surakarta. *JESI (jurnal ekonomi Syariah Indonesia)*, *11*(2), 108-114.

Darmayanti, E. S., & Wiraguna, S. A. (2025). Tanggung jawab hukum pinjaman online terhadap penyebaran data nasabah secara ilegal. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, *3*(2), 233-251.

Firmansyah, A., Falembayu, A., Siburian, A. S., Ginting, B. P., Simatupang, C., Putra, K. K., ... & Ariawan, Y. (2021). Edukasi Literasi Keuangan Kepada Kelompok Ibu-Ibu Dan Remaja Terkait Dengan Jasa Pinjaman Online Di Era Pandemi Covid 19. *Pengmasku*, *1*(1), 14-21.

https://easycash.id/blog/daftar-pinjol-ilegal

GEMINI 2.5