

Chameleon is now targeting employees: Masquerading as a CRM app

threatfabric.com/blogs/chameleon-is-now-targeting-employees-masquerading-as-crm-app



Jump to

Chameleon is back in Canada and Europe

In July 2024 Mobile Threat Intelligence analysts observed new campaigns from Chameleon, a Device-Takeover Trojan discovered back in December 2022. These campaigns introduced an unusual masquerading technique used in the campaign targeting Canada: masquerading

as a Customer Relationship Management (CRM) app. Key outtakes from the discovered campaigns are:

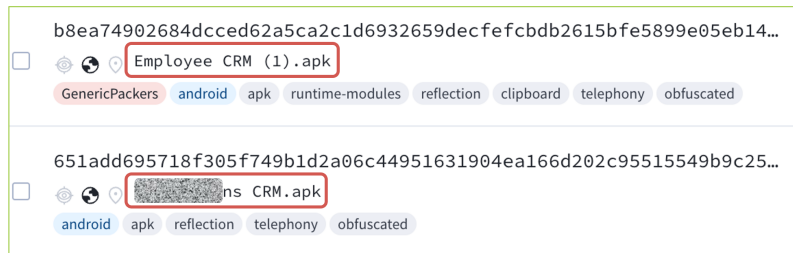
- Chameleon was seen masquerading as a CRM app, targeting a Canadian restaurant chain operating internationally
- Targeted regions include Europe and Canada, with potential further expansion of this list.
- All the samples were seen distributed with a multi-staged approach, involving a dropper bypassing Android 13+ restrictions.

New lure: targeted attack on hospitality employees

In the latest campaign discovered by ThreatFabric, Chameleon used a rather unusual masquerading technique, posing as a CRM app. At the same time, the names of the files uploaded to VirusTotal showed the targeted approach of the campaign as one of the names used the brand of a Canadian restaurant chain which operates internationally:



Chameleon: masquerading as CRM

Names of the submitted files on VT:



Samples on MTI portal:



Icon / App name / Package name
 Employee CRM (com.stub) b8ea74902684dced62a5ca2c1d6932659decfefcbdb2615bfe5899e05eb1451
 Employee CRM (com.stub) 651add695718f305f749b1d2a06c44951631904ea166d202c95515549b9c25c9

The naming used for the dropper and the payloads clearly shows that the intended victims of the campaign are hospitality workers and potentially B2C business employees in general. If the attackers succeed in infecting a device with access to corporate banking, Chameleon gets access to business banking accounts and poses a significant risk to the organisation. The increased likelihood of such access for employees whose roles involve CRM is the likely reason behind the choice of the masquerading during this latest campaign.

The first stage of the installation process involves a dropper capable of bypassing Android 13+ restrictions, which once again proves the prediction we made in the past – this capability has become essential for modern banking Trojans, and more actors have received access to the bypassing approach with the publication of the source codes of BrokewellDropper, which we reported on previously.

Once loaded, the dropper displays a fake page masquerading as a CRM login page, requesting the Employee ID. Then a message asking to reinstall the application pops up, when in actual fact it installs a Chameleon payload, bypassing Android 13+ AccessibilityService restrictions.

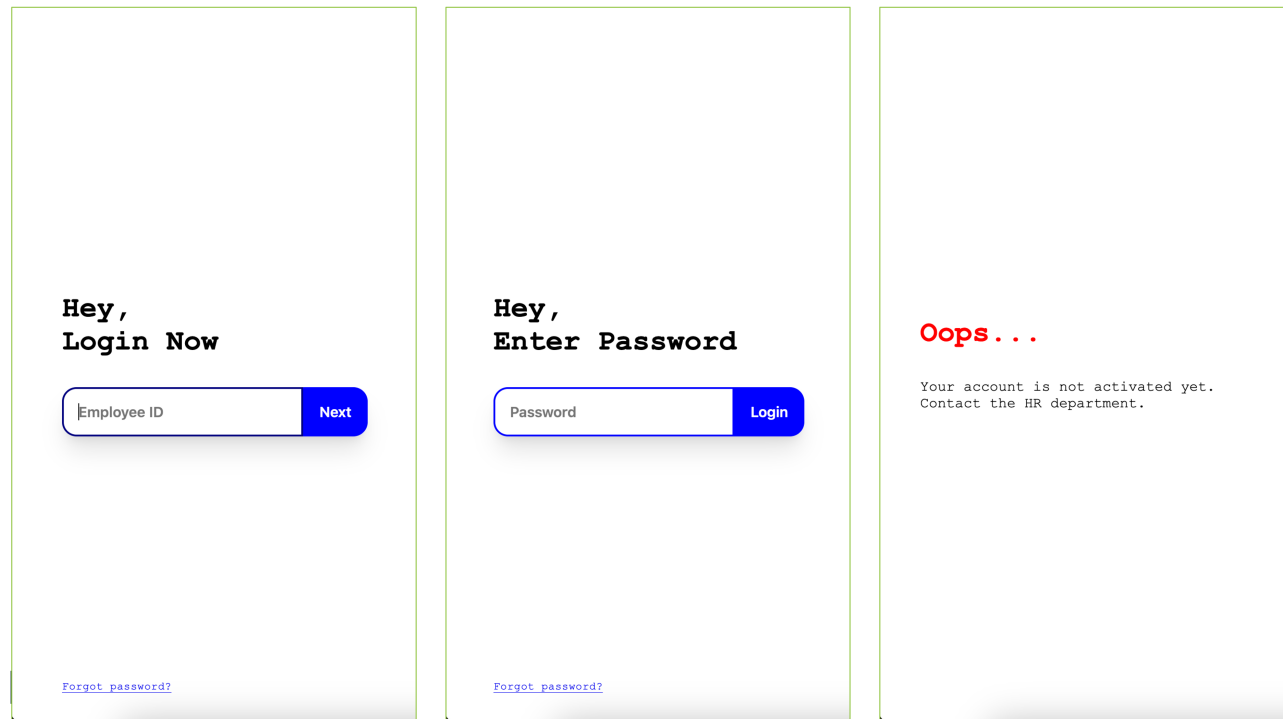
Dropper

Fake error message lures victim into initiating installing Chameleon payload



After installation, a fake website is loaded, again asking for the credentials of the employee. At the time of writing this report, after submitting the credentials, an error message was displayed.

Because Chameleon is already running in the background, it is also able to collect credentials and other sensitive information using keylogging. Such information can be used in further attacks or the actors can monetise it by selling it on underground forums.



As a part of the rising activity of Chameleon, Mobile Threat Intelligence service has also observed attacks on customers of specific financial organisations, in this case the malware was masquerading as a security app installing a security certificate released by the bank.

Conclusions

Cybercriminals tend to find original ways to target bigger assets, now targeting employees of B2C businesses and aiming to get access to business banking accounts. With the rising number of banking products for businesses (especially small and medium) and the convenience of having them available through mobile, we can expect cybercriminals to further explore the approach of targeting such mobile devices and its users. The financial organisations can take preventive steps and educate business customers about potential impact of the mobile banking malware like Chameleon and the consequences it brings landing on a mobile device with the access to business banking accounts. Moreover, with the ability to detect the presence of malware on the customer's device (especially those used to access business accounts) and spot the anomalies in activity and behaviour, banks get additional visibility to keep the customers' assets safe.