The RoamingMantis Group's Expansion to European Apple Accounts and Android Devices

By Aleksejs Kuprins

Published: 2020-06-25 · Archived: 2026-04-05 17:11:28 UTC

Background

The RoamingMantis cybercrime group has been extensively blogged about, analyzed and discussed on different information security conferences and blogs since 2017. It is known to infect victims with the following range of malware families for the Android OS: FakeCop, FakeSpy, MoqHao and FunkyBot. The malware is meant to provide the criminals with access to the victims' Android OS devices for further monetary fraud. Until now, the group has been known to focus mostly on Asian countries. It was attacking Europe back in 2018 as well, however we have found those campaigns to be not as organized as these new ones.

Press enter or click to view image in full size

The image above is present on every FakeCop malware's control panel

This trojan is usually delivered via SMS spam, containing links to a variety of different fake websites, which entice the victims to download and install a malicious component — in this case **FakeCop**.

Cases of infections via the official GooglePlay store have been identified in the past as well. Please see the references section to find the articles featuring technical analysis of each of the malware families used by this

group, as well as a summary of the group's operations and timelines.

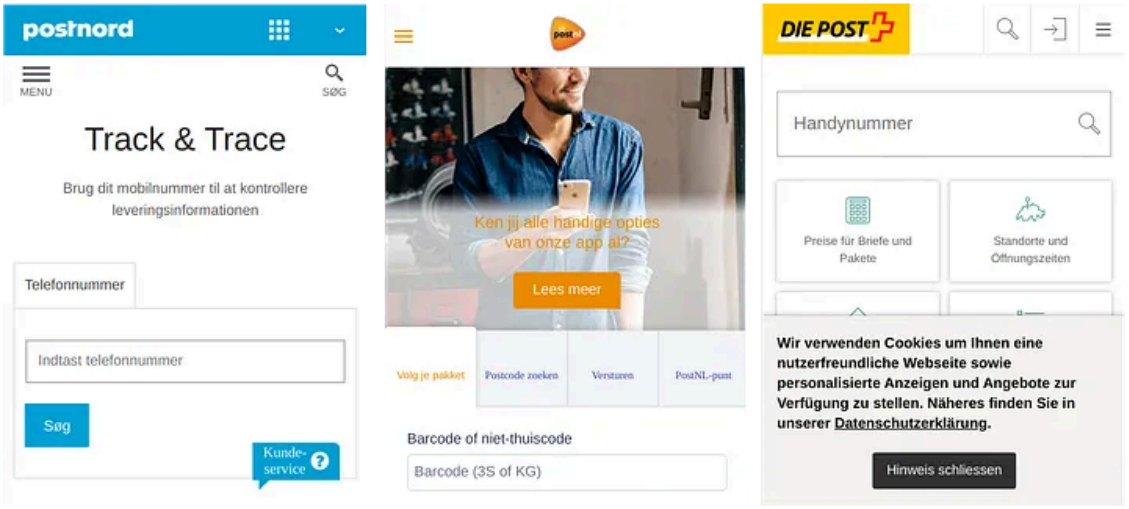
The recent events have exposed the novel ambitions of this group, particularly in their desire to extend their fraud to European countries. Specifically, we have observed such campaigns in: Denmark, France, Germany, Italy, Netherlands, Sweden and Finland. Besides these EU countries, we have also seen this attack against the mobile users in United Kingdom, Switzerland, Brazil and Japan. With this campaign, RoamingMantis is not only attacking Android OS with malware, but also employs phishing against Apple ID accounts. Please note, that unlike the Android OS component, the iOS part of the fraud is unrelated to any malicious apps.

The Move on Europe

Besides the previously used SMS spam, the chosen strategy for attacking mobile device users in these newly-added regions is the use of phishing website lures. All of these websites impersonate a locally-used postal/delivery service.

For example, the campaign in Denmark involves a website, which looks almost identical to PostNord — a postal/delivery service widely used in this country. The rest of the campaigns for the aforementioned new target countries each feature that country's own locally-popular postal/delivery service.

Press enter or click to view image in full size



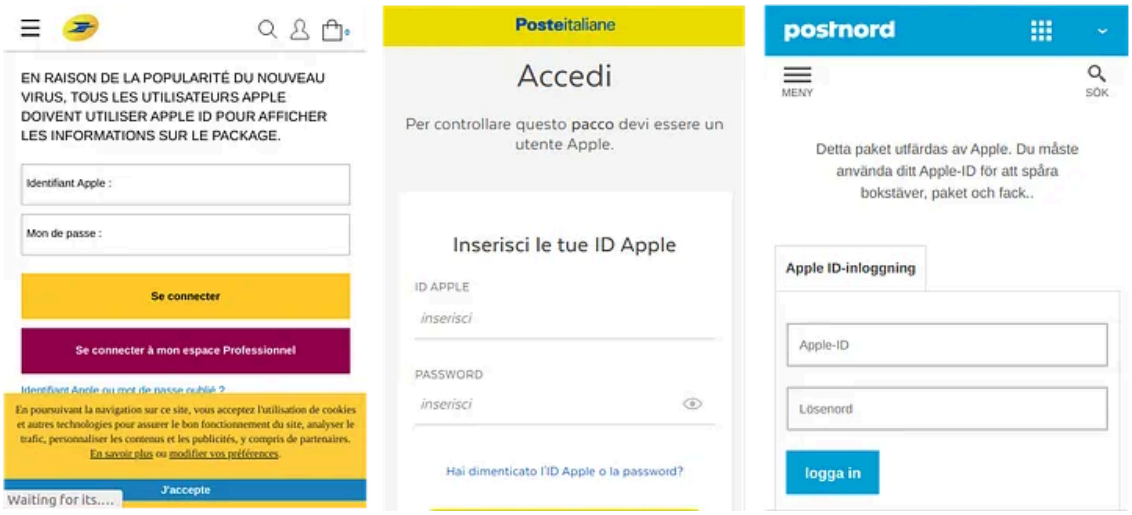
Examples of the European adaptations of the FakeCop's spreading websites

On such fake websites, the victim is usually being asked to enter their phone number. Upon entry, the website offers to download and install an APK file (APK is the file extension of app packages for the Android OS). This technique has been successfully utilized by the group in other regions in the past.

Apple ID Phishing

Along with extension to the new regions and the phishing page strategy, the RoamingMantis group has also decided to incorporate a phishing attack on the victims' Apple ID accounts.

Press enter or click to view image in full size

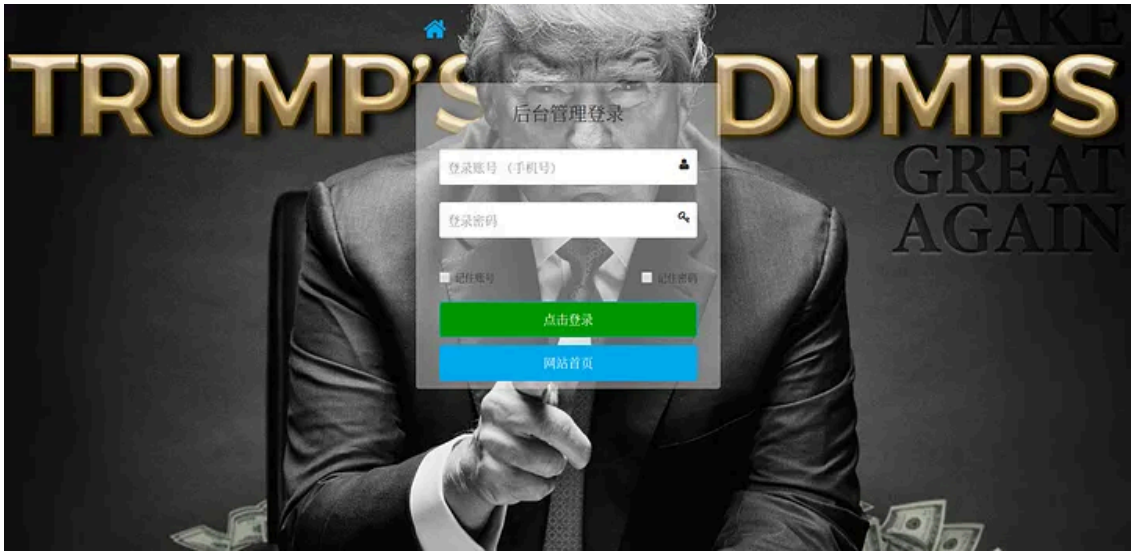


Examples of AppleID phishing pages — these are displayed to the users who run iOS

Unfortunately, the phishing pages impersonate the original websites accurately enough. For that reason, we have found these phishing pages to yield Apple ID account names and passwords to the criminals at an alarming rate. At one point we have observed the traffic of between **10 to 15** credentials **per hour, in Denmark alone**. However, this rate has slowed down greatly on the second day of our observations.

Data Collection

Press enter or click to view image in full size



The backend of RoamingMantis' FakeCop malware and its European phishing campaign is split between different hosts, each responsible for providing the criminals with a web user interface for management of the stolen data, as well as the database behind it. Each of the phishing websites runs its own panel, which stores the data acquired from the phishing.

In case anyone reading out there has looked at the screenshot above and instantly remembered an article on Krebsonsecurity about Trump's Dumps — sorry, we are not aware of any connection of RoamingMantis to it beyond the use of this design.

Press enter or click to view image in full size

Notably, all of the control panels that we have observed provide the user interface in Chinese language. It is **highly uncommon** for Chinese-speaking carders to attack European financial organizations.

RoamingMantis has a wide variety of monetization schemes, which ranges from bitcoin mining and money laundering to banking fraud. You can expect a group as large as this one to use every opportunity at their disposal to generate revenue.

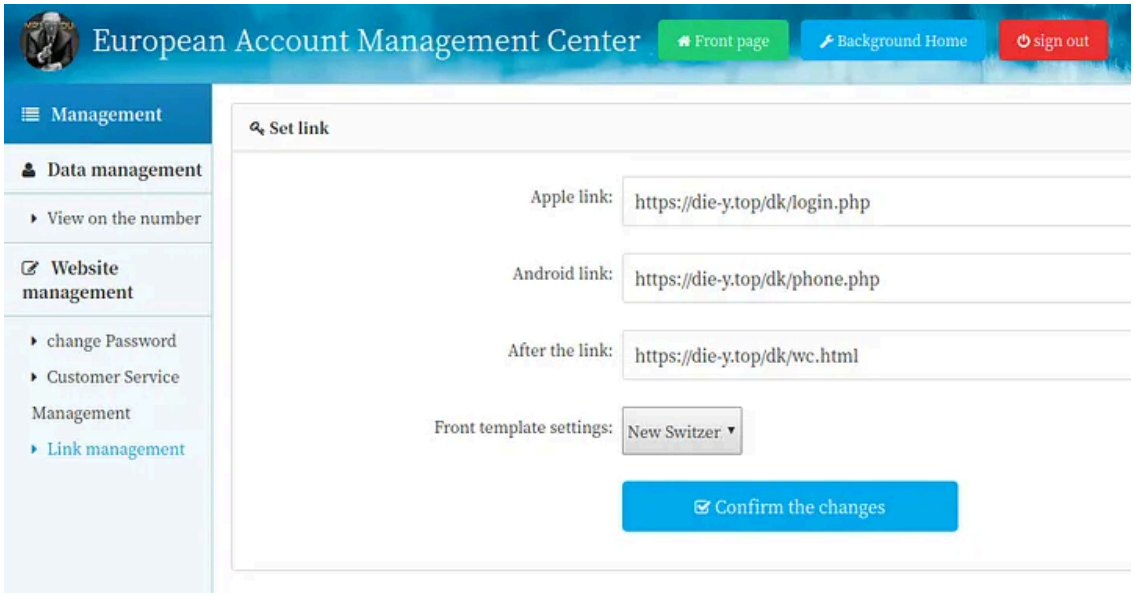
Get Aleksejs Kuprins’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

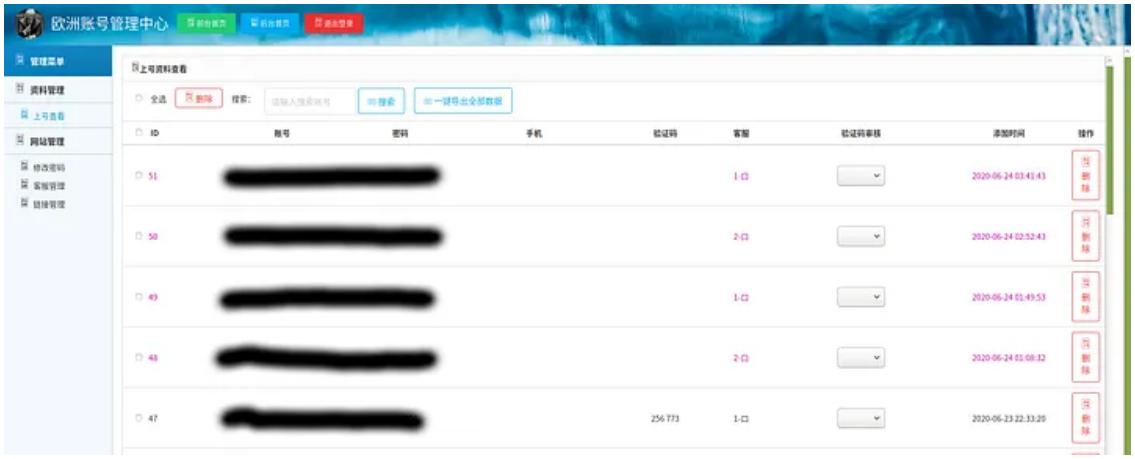
Using these control panels, the criminals can change different settings to fine-tune the phishing activity. We have used GoogleTranslate on some of the screenshots for the ease of reading.

Press enter or click to view image in full size



The Settings of the phishing website designed to attack Denmark

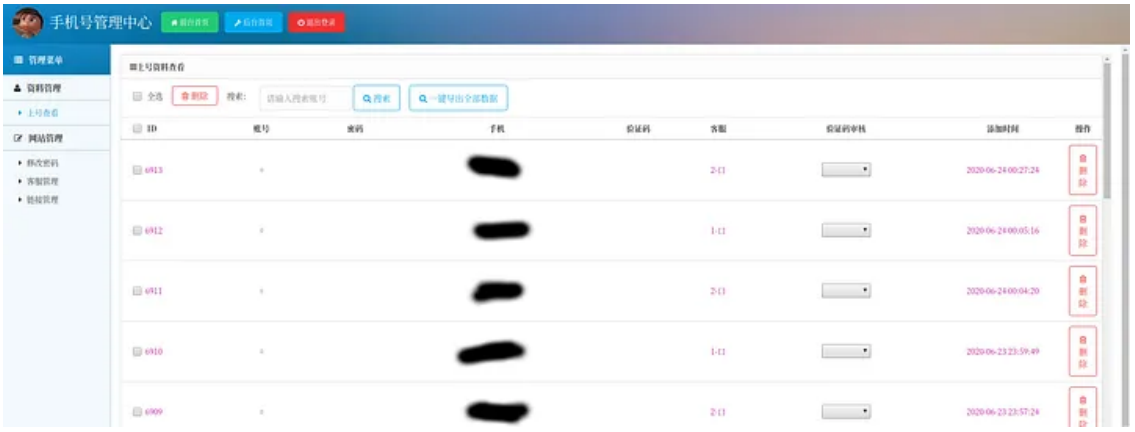
Press enter or click to view image in full size



This user interface provides the criminals with access to the stolen data from the campaign in Denmark

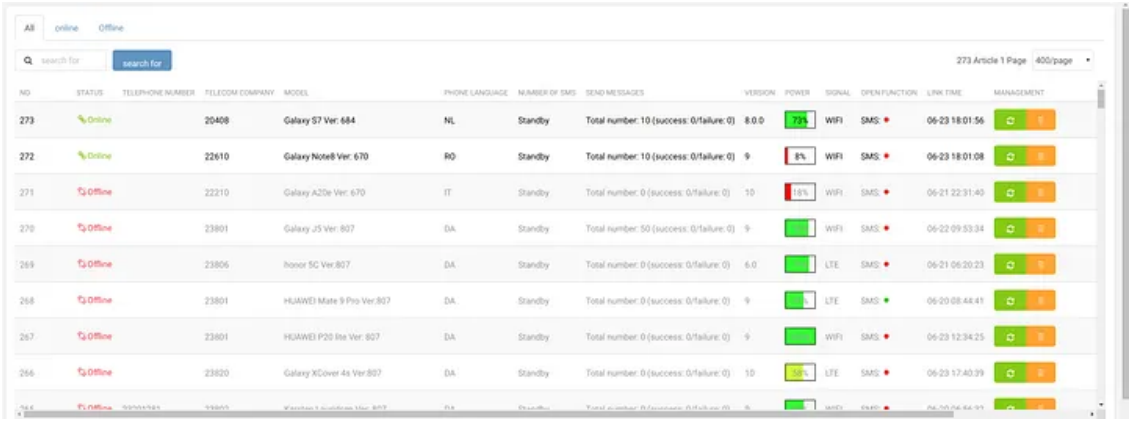
Meanwhile, the IDs of the stolen data records on the main panel are much larger, indicating its magnitude (nearly 7,000 records). This panel includes data from various campaigns:

Press enter or click to view image in full size



Finally, the user interface for monitoring of specifically the FakeCop's malware data in EU has a different design, but also shows the amount of devices affected in EU (nearly 300).

Press enter or click to view image in full size



Summary

Roaming Mantis campaigns usually come in huge volumes of spam, but now also have a wide regional coverage. The analysis above covers only a minor part of such campaigns during just two days of observation.

The technique of impersonation of postal/delivery services is nothing new and has been used rather successfully around the world by cybercriminals for years. Nearly everyone expects a package delivery from time to time and often would be impatient to receive it. The criminals will always exploit such impatience, because the phishing page can seem more credible when the victim is actually expecting a delivery.

Please remember to always verify the source of notifications for your mail or other delivery. Is it the same incoming phone number in that SMS notification as it was previously, when you have received a different delivery? Did you receive an email notification at the same time as well? Can you remember or check the official website name of your postal/delivery service? If so, maybe you could navigate to that page manually instead of clicking the provided link in the notification.

Exercise caution and avoid installing any unknown apps or entering your AppleID credentials when the context should not call for that. Your real postal/delivery service is most likely to provide their official app only through

the official app store, which is relevant for your device: Apples AppStore in case of iOS devices and Googles GooglePlay, if your device runs Android OS.

References and Further Reading

1. https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Ishimaru-Niseki-Ogawa-Mantis.pdf
2. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/
3. https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/
4. https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/
5. https://securelist.com/roaming-mantis-part-3/88071/
6. https://securelist.com/roaming-mantis-part-iv/90332/
7. https://securelist.com/roaming-mantis-part-v/96250/
8. https://blog.trendmicro.com/trendlabs-security-intelligence/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users/
9. https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/
10. https://www.fortinet.com/blog/threat-research/funkybot-malware-targets-japan
11. https://krebsonsecurity.com/2017/05/trumps-dumps-making-dumps-great-again/
12. https://twitter.com/ninoseki/status/1273057220586950656
13. https://twitter.com/ninoseki/status/1249623587574517761
14. https://twitter.com/papa_anniekey/status/1275759555830407168

IOCs

```
FakeCop APK SHA256
19e4f566c9193ab381828b390be24b63fc7c5ba32a4799bee2dc2890204f5833
1915ea279e8e5f518e766c9e3363d651891cc4e63951c1dbca0d6e600673d972
351e1cd5a9f1e39964d6ecddb81623f97ec137192cec3d314c273d31fcb4a106
359e1c533e8008969031255977493f6d07026879b7a39f3cfd4e8a3615db529f
4d008b863447590fe42cabdcf1ab5d2d9575db503a4d4566a2b298e684817fb5Phishing domains:
deutschepost .top
die-1 .top
die-5 .top
die-t .top
die-u .top
die-w .top
die-x .top
die-y .top
kuroneko-b .top
kuroneko-c .top
kuroneko-d .top
kuroneko-e .top
kuroneko-f .top
kuroneko-h .top
```

```
kuroneko-i .top
kuroneko-k .top
kuroneko-m .top
kuroneko-n .top
kuroneko-o .top
kuroneko-r .top
kuroneko-u .top
kuroneko-x .top
laposet .top
poste-m .com
postnl .top
royal-mail .top
www.postnl .top
post-y .top
fr-a .top
post-ap .top
jppost-tu .top
jppost-ha .top
jppost-hi .top
jppost-ru .top
jppost-yu .top
jppost-ka .co
jppost-ama .com
jppost-so .co
jppost-ke .co
jppost-si .co
jppost-ki .co
jppost-ko .co
jppost-so .top
jppost-sso .topHost/C2 IPs:
103.126.100 .18
103.145.106 .131
45.137.183 .33
```

Source: https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681