People infected with coronavirus are all around you, says Ginp Trojan

By Alexander Eremin

Published: 2020-03-24 · Archived: 2026-04-10 02:53:15 UTC

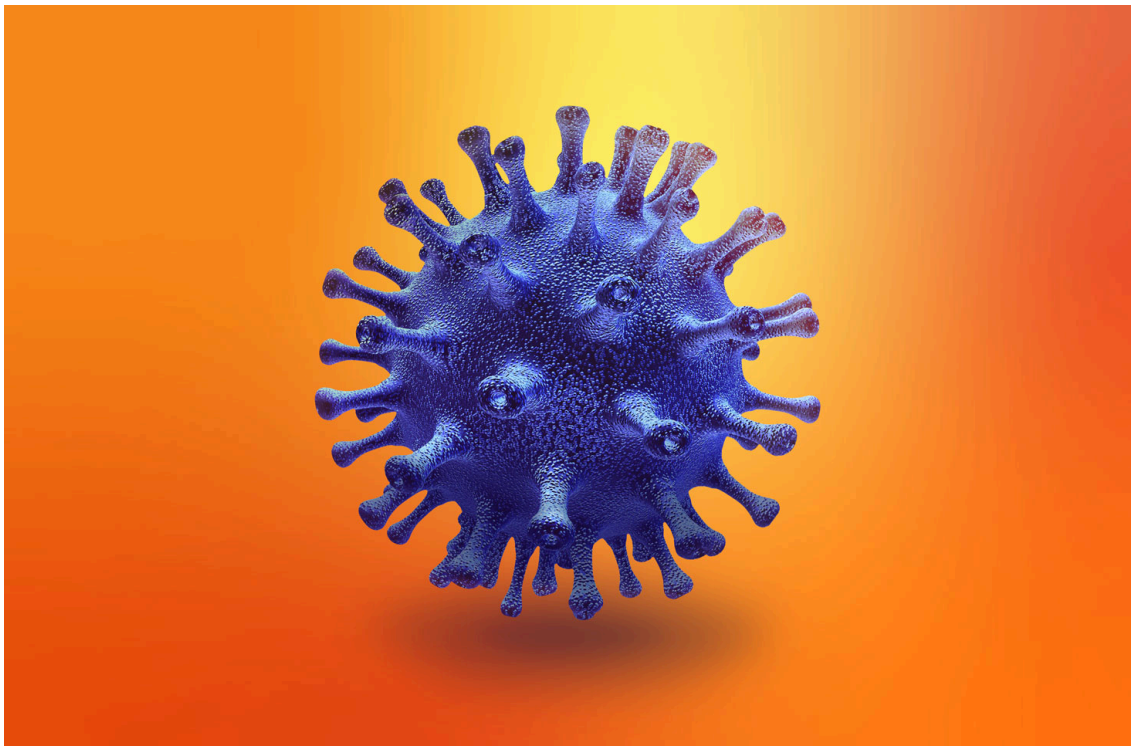
- coronavirus

Ginp banking Trojan uses information about people infected with coronavirus as bait to lure Android users into giving away credit card data.

- 

  Alexander Eremin

- March 24, 2020

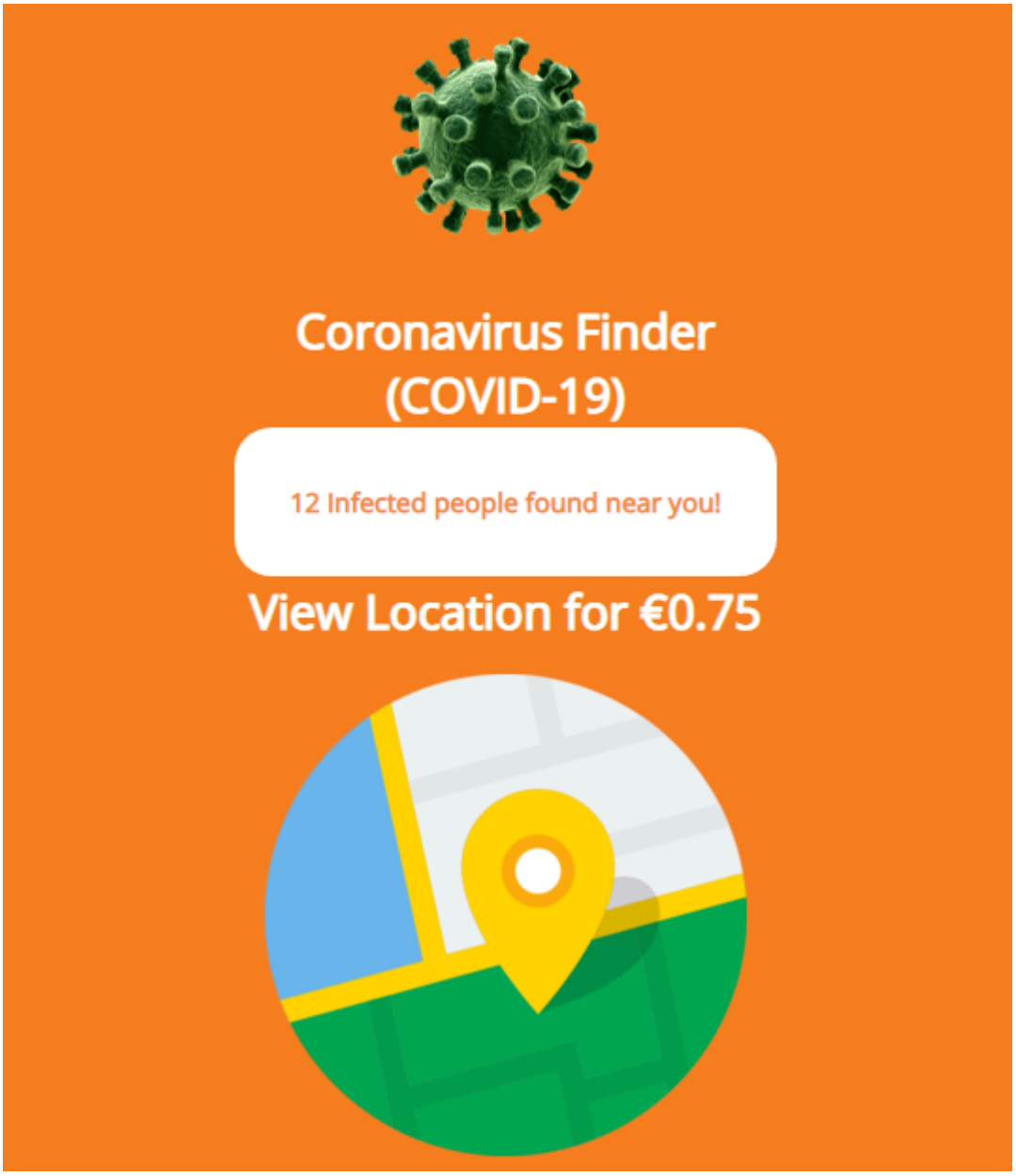


As people all around the world started working from home and practicing social distancing, the latter in some cases may evolve into paranoia. Should I avoid contacting everyone, because, who knows, maybe this person has

contracted the coronavirus. Or maybe that one? People became somewhat afraid of all other people. And cybercriminals decided to make use of that.

The Coronavirus Finder (that doesn't work)

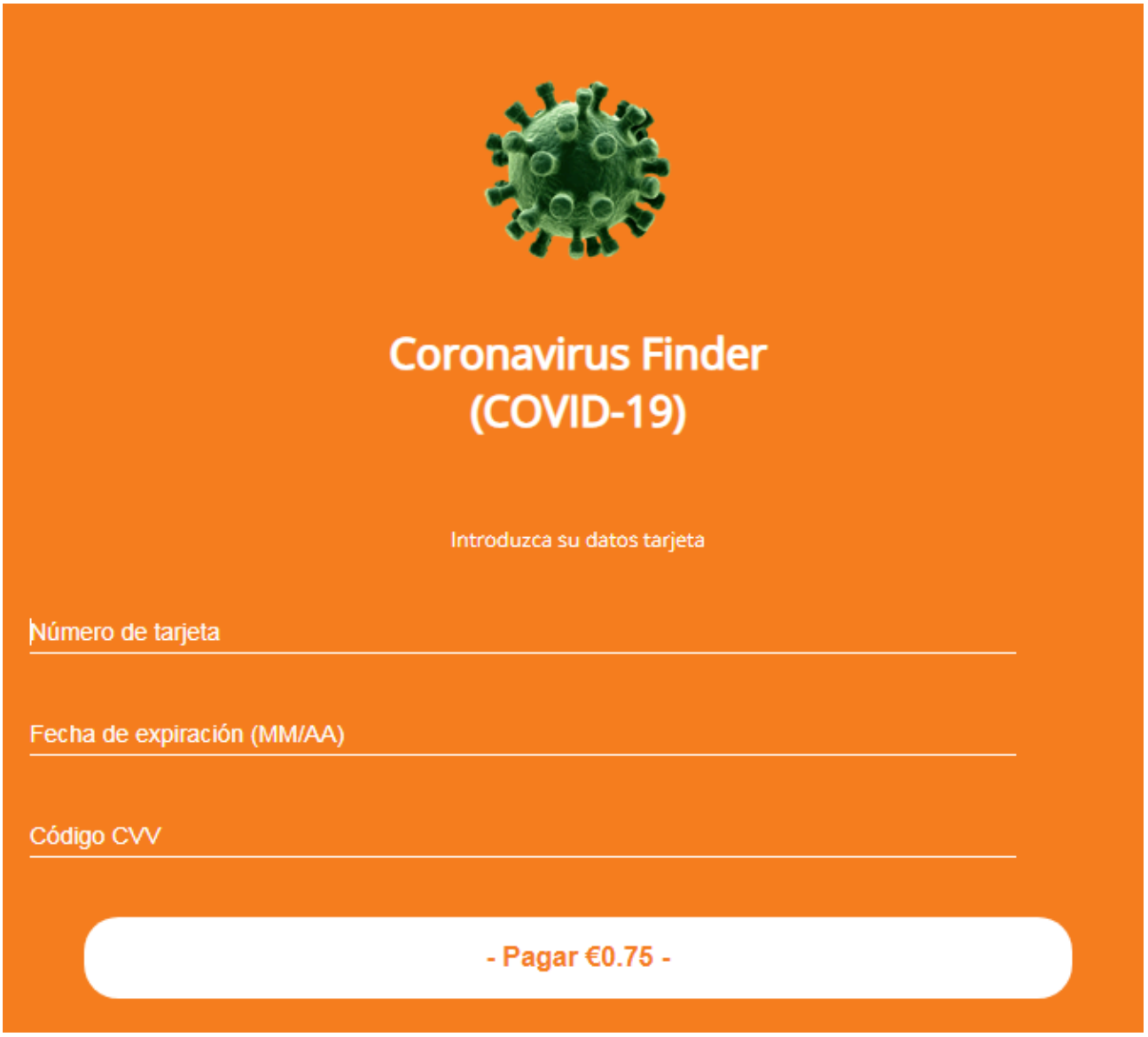
Cybercriminals behind Ginp, a banking Trojan that we have covered recently (here's a post about Ginp on Kaspersky Daily), are up to a new campaign related to COVID-19. After Ginp receives a special command, it opens a web-page called Coronavirus Finder. It has a simple interface that shows the number of people infected with the coronavirus near you and urges you to pay a small sum to see the location of those people.



Oh, what a relief for some people would it be to know whom to avoid! For some people, the message looks more than convincing, so they proceed to pay the fee. The amount seems to be quite small, so it's easy to spare. The web-page then offers you to input your card data to make the transaction.

As you may remember, Ginp is a very capable banking Trojan that relies on a lot of different lures to make users input their credit card data into forms, so that it can steal it. If you guessed this web-page is just another form aimed at stealing data — you've guessed it right!

Once you fill in your credit card data, it goes directly to the criminals… and nothing else happens. They don't even charge you this small sum (and why would they, now that they have all the funds from the card at their command?). And of course, they don't show you any information about people infected with coronavirus near you, because they don't have any.



Given the speed at which the virus spreads, no one has such information, even the governments. So don't fall for this lure. What's more, to see such a web-page pop up on your device, you need to have Ginp on it first. As long as you're protected and don't have a Trojan Horse on your phone, you won't be seeing such notifications.

According to data from Kaspersky Security Network, most users who have faced Ginp, are located in Spain, just as before. However, this is a new version of Ginp that is tagged "flash-2", while previous versions were tagged "flash-es12". Maybe the lack of "es" in the tag of the newer version means that cybercriminals plan to expand the campaign beyond Spain.

That's not the first time we've seen cybercriminals exploit the coronavirus topic. They've already used it as bait in phishing messages and created coronavirus-themed malware.

Staying safe from Ginp banking Trojan

Our advice on how to stay safe from Ginp Banking Trojan remains the same:

- Download apps only from Google Play (and disable the option to install apps from other sources).
- Stay skeptical. If something seems suspicious – don't click and, most importantly, don't give any sensitive data such as logins, passwords and payment credentials away.
- Do not give the Accessibility permission to apps that request it, other than anti-virus apps.
- Use a reliable security solution. For example, is quite aware of Ginp and detects it as Tojan-Banker.AndroidOS.Ginp.

For staying safe from the coronavirus, we suggest that you follow the WHO's guidelines.

Protecting health care

Health-care facilities are struggling with the current coronavirus epidemic, so we must help them with cyberprotection. We are offering free six-month licenses for our core solutions.

Tips

Is your security system secure?

Protecting a security console is more critical than one might think. Here’s the lowdown on control-layer compromise, and how to keep it from happening.
