Indonesian Magecart hackers arrested

sansec.io/labs/2020/01/25/magecart-hackers-arrested/

January 25, 2020

- 25th January 2020

  Web Skimming / Sansec Threat Research
  Learn about new eCommerce hacks?

  Receive an alert whenever we discover new hacks or vulnerabilities that may affect your online store.

- What is
  Magecart?

  Also known as digital skimming, this crime has surged since 2015. Criminals steal card data during online shopping. Who are behind these notorious hacks, how does it work, and how have Magecart attacks evolved over time?

  About Magecart

photo by Oktarina Paramitha Sandy

The Indonesian police announced on Friday that they have arrested three alleged Magecart hackers on December 20th. The suspects are from Jakarta and Yogyakarta and are 23, 26 and 35 years old. After the press conference, one suspect admitted on Indonesian

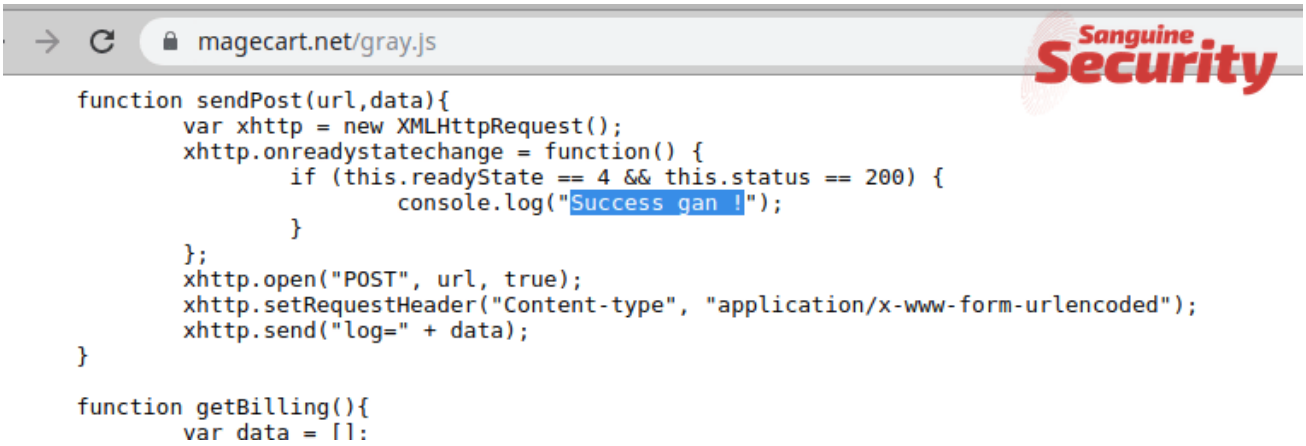
television that he had injected web skimmers into ecommerce stores since 2017 and only made enough money to “buy a jacket”. The suspects face up to 10 years in prison under article 363 of the Indonesian Criminal Code.

The Indonesian police reported that this group had intercepted payments for 12 (mostly European) stores. The arrests carried out by Indonesian police were part of a coordinated Interpol anti-skimming campaign called **Operation Night Fury** with support from European and US cyberteams.

> Joint press conference by Indonesian National Police & #INTERPOL on Operation Night Fury led by INTERPOL’s #ASEAN Desk, sharing the successful arrest of 3 suspects involved in JS-sniffer campaign compromising e-commerce websites to steal credit card or online payment information pic.twitter.com/2C12fvZ92X
>
> — INTERPOL_Cyber (@INTERPOL_Cyber) January 24, 2020

571 stores hacked, suspects still at large

Sansec has been tracking the activity of this group for several years and has identified not 12 but 571 hacks by the same individuals. These hacks could be attributed because of an odd message that was left in all of the skimming code:



“Success gan !” translates to “Success bro” in Indonesian and has been present for years on all of their skimming infrastructure.

The hackers registered a range of domain names for their skimming operations, some of them clearly referring to their whereabouts or intentions. Here is a small sample:

```
trustme.web.id
bikin.id
nganuenak.com ("delicious")
bakulsemprul.com (a cafetaria on Kalimantan)
adventurewar.com
ride4speed.com
magecart.net
```

Furthermore, we have observed similar hacks since the arrest at December 20th. The Indonesian police confirms that suspects from the same group are still at large, but would not disclose further details. As of today, we found 27 stores that are still being skimmed using the same code. Several exfiltration servers are still actively collecting intercepted payments, notably the brazen `magecart.net` domain.

End of Magecart?

This group had a serious impact on global ecommerce security in recent years, by skimming at least 571 hacked stores. However, they were responsible for just 1% of all Magecart incidents since 2017. Sansec estimates that there are yet another 40 to 50 more sophisticated individuals involved in web-skimming activity.

About us

Sansec was the first to publish about web skimming and has been tracking global skimming activity since 2015. Our anti-skimming technology and fraud data are used by merchants, forensic investigators, financial anti-fraud teams and service providers.

Get in touch!

data-size="large" > Follow @sansecio