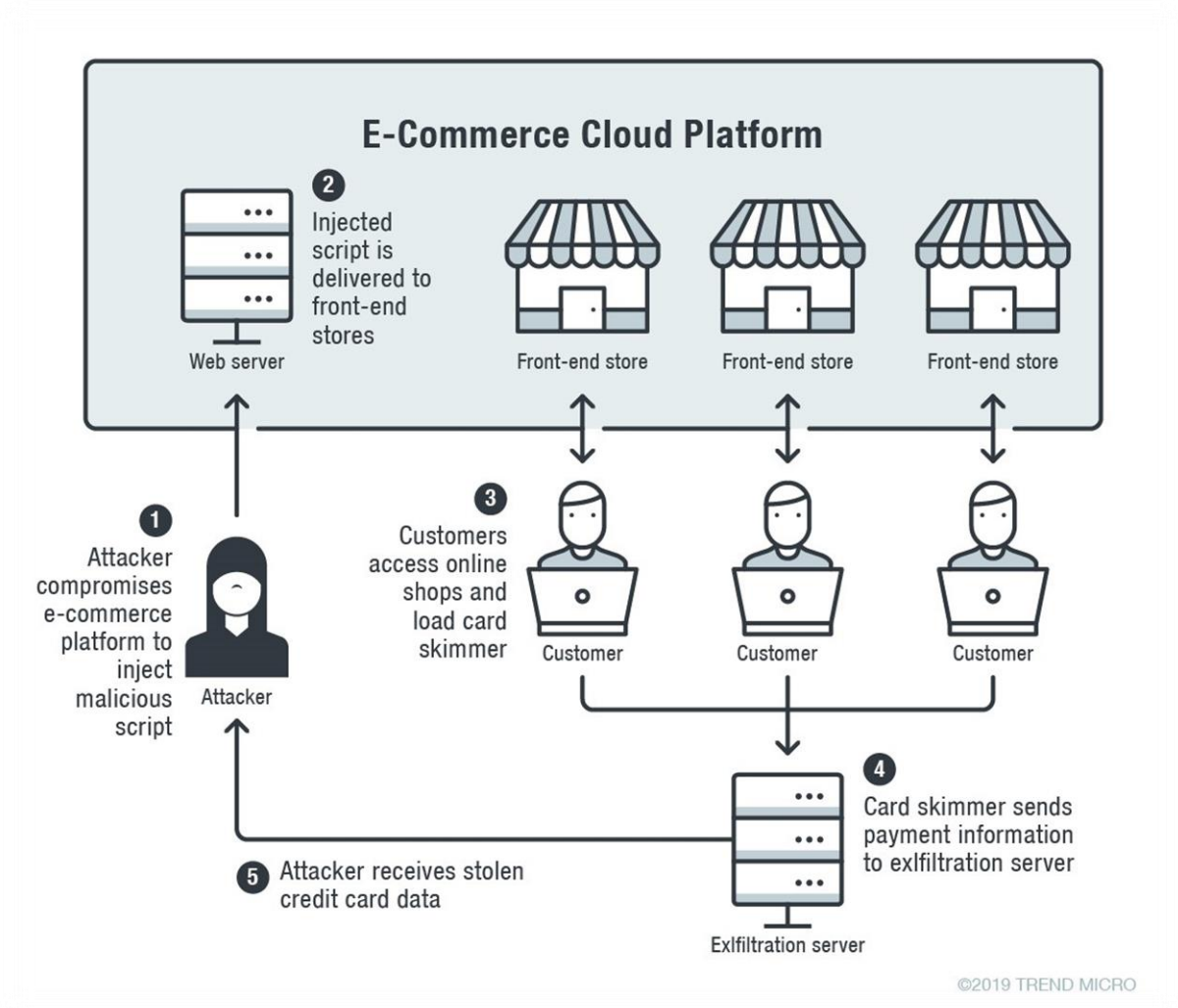
MAGECART RECENT ACTIVITIES

MageCart is a cybercriminal group which consists of more than 10 distinct groups are responsible for digital credit card skimming on many compromised websites also well-known with high-profile breaches of global brands like Ticketmaster, British Airways and Newegg. They are placing their javascript digital credit card skimmers which is called with again their own name as magecart.js on compromised websites in order to steal user's credit cards information by copying input fields from website and send it to command and control servers. Each group in MageCart has its own unique ways and methods to compromise websites, like while Group-5 is searching third party suppliers to breach as many victims as it can, Group-4 finds the best methods to hide themselves in a compromised website. According to findings on many reports, MageCart is thought responsible for a great number of known and unknown data breaches even just in 2020.



MAGECART RECENT ACTIVITIES

Samples from Attacks of MageCart

Source	Targets	Release Date	Report
GEMINI	Multiple	July 2020	Click for report
SUCURI	Unknown	July 2020	Click for report
RISK IQ	Multiple	September 2020	Click for report
TREND MICRO	US Local Government Services	June 2020	Click for report
SANSEC	Intersport, Claire's, and Icing Websites	June 2020	Click for report
TREND MICRO	Multiple	October 2020	Click for report
MALWAREBYTES LAB	Multiple Unknown Found skimmers on Amazon CloudFront CDN	June 2019	Click for report
MALWAREBYTES LAB	Multiple – Found GitHub library used to compromise multiple targets	April 2019	Click for report
RISK IQ	Ticketmaster	June 2018	Click for report
RISK IQ	British Airways / 380.000 Victims	September 2018	Click for report

These are the just well-known examples from lots of different data breaches of MageCart and there are lots of others like we noticed above. So, it seems these kinds of attacks will have been continued and we have to consider the best ways to prevent them or at least minimize the number of attacks even if it is not possible to prevent completely.