# Magecart cybercriminals leveraging public WiFi vulnerabilities

Reference: Memo [191004-1] – Version: 1.0
Keywords: cyber-crime, Magecart, routers, e-commerce, digital services, supply chain compromise
Sources: Publicly available information

## Key Points

- Cyber-criminal groups dubbed Magecart are exploiting vulnerable e-commerce websites to steal user payment data.
- One Magecart group has tested methods to compromise user devices browsing the internet via public WiFi hotspots.
- The same group is also attempting to compromise code used by mobile app developers and affect a large user base.

## Summary

Since at least September 2018, cyber-criminal groups designated under the umbrella name Magecart have been exploiting vulnerabilities in electronic payment systems, and more specifically the Magento payment software that powers many e-commerce websites, to gain access to customer credit card information in a technique known as card skimming.

Recently, research by IBM[1] revealed that the Magecart group 5 (MG5) was testing code designed for injection into benign JavaScript (JS) files loaded by routers that support the layer 7 (L7) protocol. L7 is typically used in commercial-class routers because it has the ability to balance internet traffic loads, ensure quality of service and support displaying an ad page while users connect to a WiFi service's central portal. Such routers typically support "free and fee" WiFi access in large public areas such as hotels and airports. In such places, WiFi services are often outsourced, and operators sometimes offer a discount if hotels or airports allow ads to run before guests connect. In such a scenario, MG5 infected L7 routers could inject malicious ads that would compromise users wishing to connect the internet.

According to IBM research, this method is currently only being tested by attackers, and no live deployment has been observed. If attackers proceeded to exploitation in the wild, they could leverage the compromised routers in two ways:

- Steal users' payment data when they browse e-commerce sites through a compromised router; and
- Inject malicious ads into webpages viewed by all connected guest devices, including those who pay to use the internet and those connecting to a hotel's free WiFi hotspots.

IBM researchers also found that MG5 has infected some instances of open-source mobile app code that is offered to app developers for free. If deployed, this infected code could allow to compromise data belonging to app users.

## Comments

Online credit card data skimming is an old technique used by cybercriminals. According to RiskIQ and FlashPoint[2], in April 2000 it was revealed that the Cart32 shopping cart software had been backdoored for more than a year, exposing the credit card information of thousands of e-commerce customers. In December 2013, the Magento payment software was reportedly compromised for the first time. By 2015, the Magecart group began injecting skimmers into vendors' websites and, in 2016 a second group emerged, with a skimmer and infrastructure distinct from the first group.

By September 2018, this threat became widely known when British Airways announced it had suffered a breach resulting in the theft of payment data of 380,000 customers. Since then, IT security experts have found that at least 12 groups have been reusing similar malicious web-skimming code.

To deploy their payment data skimmer code, Magecart groups leverage the numerous dependencies in the e-advertisement / e-commerce eco-system, a form of supply chain compromise. For example, in late 2018, the Magecart group 12 reportedly compromised a content delivery network for advertisements, so that any website loading script from the ad agency would inadvertently serve a Magecart skimmer to visitors.

Many organisations worldwide have been affected by Magecart attacks, while at user level they have even been detected at EU-I. The most recent techniques tested by MG5 demonstrate that the groups continue to evolve and learn in order to steal payment data from an ever-larger number of victims.

The responsibility to mitigate these attacks lies primarily on the e-commerce operators. They should avoid using unverified third-party code and implement integrity checks for any JS files loaded from third-party providers.

[1] https://securityintelligence.com/posts/leading-magecart-group-targeting-captive-wi-fi-users-via-l7-routers/
[2] https://go.flashpoint-intel.com/docs/inside-magecart-by-Flashpoint-and-RiskIQ