

Scammers try a new way to steal online shoppers' payment-card data

reader comments

9 with 9 posters participating

Share this story

Thieves have devised a new way to steal payment-card data from online shoppers—or at least it's new to the researcher who found it. Rather than infecting a merchant's checkout page with malware that skims the information, the thieves trick users into thinking they've been redirected to an authorized third-party payment processor.

So-called payment-service platforms are common in the world of ecommerce, particularly for smaller sites that don't have the resources to harden their servers against sophisticated attacks. That includes the rash of hacks coming from so-called Magecart groups that target the Magento ecommerce Web platform. Rather than assuming the considerable risk of hacks that steal passwords, payment card details, or other sensitive data, sites can offload the payment card charges to experienced PSPs.

Jérôme Segura, head of threat intelligence at security provider Malwarebytes, said he recently found an attack that targets sites that use this type of arrangement. By infecting the merchant site and adding a line or two of code, the attackers redirect users to a fake PSP rather than the

legitimate one, at the time of purchase. The ruse works similarly to a phishing attack. Graphics that mimic real services, custom-created domain names, and other sleights of hand trick end users into thinking they've landed on a genuine third-party processor.

Convincing replica

Enlarge / A compromised merchant website redirects shoppers to this fake third-party processor.

Malwarebytes

"This is simply a way for them [the attackers] to adjust to whatever method of payment an ecommerce site uses," Segura wrote in an email. "If the merchant takes payments themselves, they [the attackers] will use the typical skimmer that looks for specific fields, and if the merchant instead relies on an external payment gateway, they can deploy that fraudulent page designed like a phish to collect the data."

A compromised merchant website redirects shoppers to this fake third-party processor.[/ars_img]So far, Segura has found only one instance of this ruse. It compromised an online store in Australia that used the PrestaShop content-management system. As the image to the right shows, the fake PSP was hosted at payment-mastercard[.]com. The side-by-side comparison below

shows how carefully it mimicked Australia's Commonwealth Bank, which was the authentic PSP for the online merchant. Under the hood, however, the fake one harvested the payment-card data so it could be used in fraudulent transactions.

Enlarge / A side-by-side comparison shows how similar the fake processor looks to the real one.

Malwarebytes

"The scheme consists of swapping the legitimate e-banking page with the fraudulent one in order to collect the victims' credit card details," Segura explained in a post published on Thursday. "We also noticed that the fake page did something we don't always see with standard skimmers in that it checked that all fields were valid and informed the user if they weren't."

Once the fake PSP has collected the data, it redirects buyers to the legitimate PSP and includes the purchase amount.

While Segura is aware of only one active attack using this method, he believes it may be a trial run before the scammers start more widespread scams. He said he has seen one skimmer group create dozens of domains that resemble legitimate banking institutions. He previously wondered why skimmers would bother. After seeing the attack against the Australian

merchant, he said he may have found the reason.

One of the few ways for users without a background in online security to detect this type of scam is to take note of the fake PSP redirecting to the real one after accepting the payment card data. Someone who is truly attentive will not only notice that the card data is being sought for a second time. They will also notice the difference in the domains between the two services (see the side-by-side comparison above). Malwarebytes antivirus—and possibly other security programs—make detection easier by automatically flagging the fake PSP. Thursday's post also provides indicators of compromise people can use to determine if they've been targeted.

<https://arstechnica.com/?p=1622093>