

A new rash of highly covert card-skimming malware infects ecommerce sites



reader comments

35 with 29 posters participating

Share this story

The rash of e-commerce sites infected with card-skimming malware is showing no signs of abating. Researchers on Thursday revealed that seven sites—each with more than 500,000 collective visitors per month—have been compromised with a previously unseen strain of sniffing malware designed to surreptitiously swoop in and steal payment card data as soon as visitors make a purchase.

One of those sites, UK sporting goods outlet Fila.co.uk, had been infected since November and had only removed the malware in the past 24 hours, researchers with security firm Group-IB told Ars. The remaining six sites—jungleeny.com, forshaw.com, absolutenewyork.com, cajungrocer.com, getrx.com, and sharbor.com—remained infected at the time this post was being reported. Ars sent messages seeking comment to all seven sites but has yet to receive a response from any of them.

Group-IB has dubbed the JavaScript sniffer GMO after the gmo[.]il domain it uses to send pilfered data from infected sites, all of which run the Magento e-commerce Web platform. The researchers said the domain was registered last May and that the malware has been active since then. To conceal itself, GMO compresses the skimmer into a tiny space that's highly obfuscated and remains dormant when it detects the Firebug or Google Developer Tools running on a visitor's computer. GMO was manually injected into all seven sites, an indication that it is still relatively fledgling.

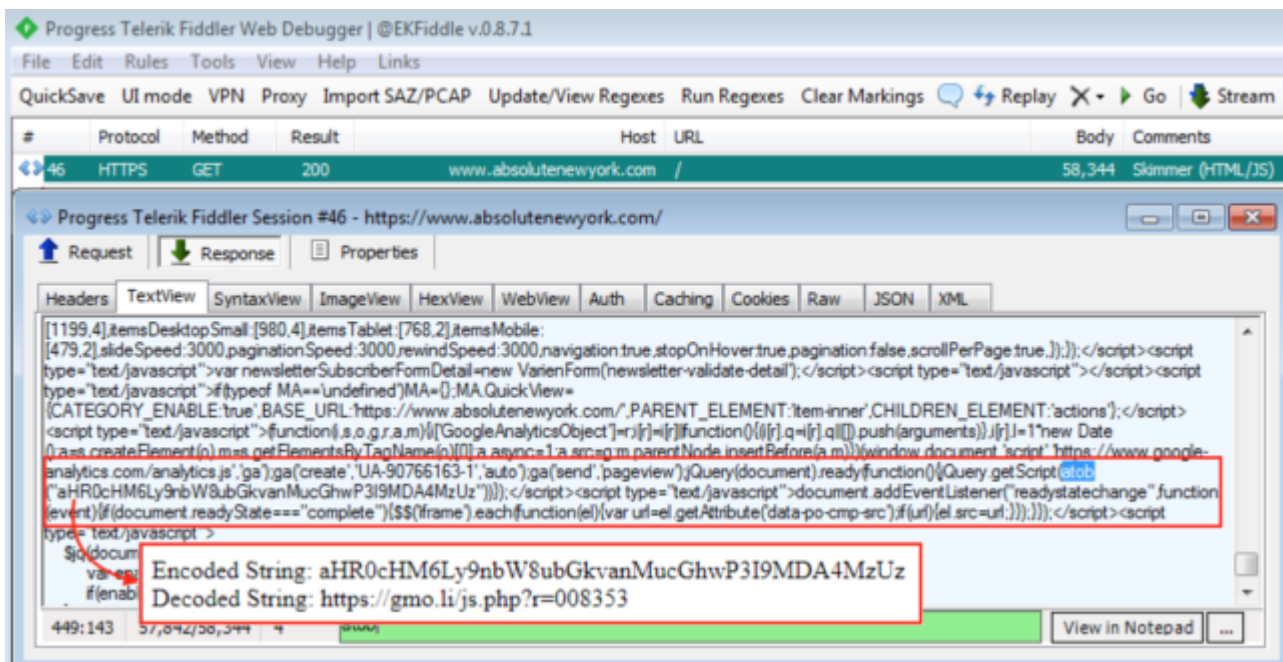
The Magecart crime bonanza

Group-IB's discovery comes six months after similar card-skimming JavaScript infected British Airways, Ticketmaster, and other popular websites. Since then, researchers have uncovered a raft of competing crime gangs that specialize in infecting big-name sites that accept payment-card data from visitors. RiskIQ, a firm that researched the site infections early on, gave the name Magecart to the 12 distinct groups it identified as targeting weaknesses in Magento.

In a testament to just how popular the crime has become, a researcher from security provider Malwarebytes in November found a single site that was infected by two different card skimmers. In an email Thursday, Jérôme Segura—the Malwarebytes researcher behind that finding—noted a Brazilian Fila website was previously found to be infected and that some of the

domains used in the attack were the same as ones found in the compromise he discovered.

Segura went on to say Group-IB's findings were consistent with this archived scan of the Fila UK site and the screenshot below, which he took Thursday morning while visiting absolutenewyork.com.



Jérôme Segura

The rise of card-skimming malware infecting popular sites comes as the plummeting price of cryptocurrencies has left criminal hackers scrambling for new sources of revenue. Through a company spokesman, Nicholas Palmer, vice president of international business at Group-IB, told Ars that GMO is one of the 15 families of sniffers Group-IB has recently discovered and plans to detail in an upcoming research paper. Thursday's report indicates that the Magento-style crime wave is showing no signs of slowing down.

"People should understand that, despite its simplicity, JS Sniffers shouldn't be underestimated," Palmer told Ars. "Ticketmaster, British Airways, and Fila proved that any e-commerce business around the world is vulnerable to this type of attack. And not only online stores get affected, but also payment systems and banks whose clients suffer from payment

data leaks.”

One of the keys to the recent card-skimming successes is the difficulty both end users and sites experience in detecting the malicious JavaScript. The logos many e-commerce sites display certifying that the site is secure are meaningless, as are most of the payment-card industry rules imposed on merchants. While credit and debit cards are protected against fraud, the hassle involved in recouping losses and replacing compromised cards still makes the thefts painful.

People who make a fair number of online purchases may want to consider using temporary cards that have small, fixed lines of credit. All payment-card users should carefully check their statements every month for fraudulent charges.

<https://arstechnica.com/?p=1474033>