




Tech Vulnerability Management

 E-mail this page |  Print this page |  BOOKMARK 

Mariposa Botnet Operators Didn't Bite In 'Cookie-Stuffing' Offer

Ecommerce fraud technique steals commission, referral fees from website affiliates

Aug 26, 2010 | 02:27 PM | [0 Comments](#)

By Kelly Jackson Higgins

The Slovenian man recently arrested for allegedly writing the malware used to build the now-infamous Mariposa botnet also sold an additional feature for his bot software, a form of cookie fraud known as "cookie-stuffing."

According to the researcher who helped take down Mariposa, the Spanish operators who purchased the bot software from the Slovenian man known as "Iserdo" and then built Mariposa, for some reason didn't opt for the feature, which he offered for 200 euros, even though it would have increased their potential profits. "That was one module they didn't buy," says Luis Carrons, technical director of PandaLabs, which teamed up with the FBI, Defence Intelligence, and Georgia Tech [to derail the botnet](#) in December of last year. "The most likely explanation is that they didn't even know what it was about. Otherwise, they could have multiplied the profit they were doing."

Mariposa, a massive global botnet that infected close to 13 million machines in more than 190 countries, harvested banking credentials, credit card information, account information from social networking sites and online email services, and other usernames and passwords.

Cookie-stuffing would have added another revenue stream for the Mariposa operators. This often-overlooked but lucrative form of crime is where a fraudster sticks his own cookies atop legitimate cookies planted for affiliate marketing purposes. Websites with affiliate programs pay commission to those affiliates, such as reward sites, for bringing in customers who ultimately conduct transactions on the site.

But a cookie-stuffing attack ensures that fraudster gets the commission, not the affiliate. So if a customer who visited an affiliate site infected with cookie-stuffing purchases an antivirus package from an AV vendor, his compromised purchase cookie would instead credit the bad guy and force the website to pay the bad guy the commission rather than the legitimate affiliate. "The final user [customer] doesn't notice it, as he is not charged

Vulnerability Management Reports



Endpoint Security: Winning the Endgame
 Sophisticated malware is proliferating, especially at the endpoints. Here's what you need to know about protecting your PCs, laptops and other endpoints in the new security arms race.



Why "Free" Patch Management Tools Could Cost You More
 Free, native patch management tools may look attractive at first, but closer inspection reveals hidden costs and missing capabilities. The result is fragmented patch management and weaker security, which is costly and cumbersome. Learn why "free" can cost more than you think.



Patch Management: Pick the Low-Hanging Fruit
 Fixing third-party application vulnerabilities is at the core of sound information security. Learn how to make sure patch management is optimizing your security posture.

Other reports from the Vulnerability Management Tech Center:

- Five Key Factors for Endpoint Management and Security Suites
- Three Strategies to Protect Endpoints from Risky Applications
- Security Pro's Guide to Patch Management
- In-House Malware Analysis: Why You Need It, How to Do It
- Scanning Reality: Limits of Automated Vulnerability Scanners
- Using BSIMM To Develop Safe Applications
- Applications Security: Eliminating Vulnerabilities in Enterprise Software
- In a Fix? Try a Vulnerability Remediation Life Cycle
- Sharing Is Daring: Multi-Enterprise Vulnerability Management Strategies
- Compliance 101: Creating a Strong Vulnerability Management Strategy
- Ground Zero: Building a Layered Defense Against Unknown Threats
- Assessing the Danger: How IT Can Ace Vulnerability Management

more money for his online purchases. The real affiliates will think that the user has not bought any items, and that's why they're not getting their commission. And some sellers will be even be really happy thinking that they have a very active affiliate," explains Carrons.

Websites rigged with cookie-stuffing often don't even know it. Carrons says cookie-stuffing may be responsible for stealing millions of dollars on a daily basis. "The truth is that nobody is able to calculate the amount of money that is being stolen using this technique, mainly because [sites often don't] realize that the robbery is taking place. But for sure it is in the millions at least," Carrons says.

An executive from a Spanish airline recently told Carrons that his company had discovered that it was actually paying hundreds of thousands of euros per month to a Turkish man located in Germany. "They were sure he was practicing cookie-stuffing, but they couldn't prove it," Carrons says.

Cookie-stuffing attacks have been used for years, he says. "I've been tracking this for more than a year now, but unfortunately it is not that easy to find out a way to measure this fraud. The good news is that the affiliate networks are already aware of this problem, and most of them have their license agreements, and the final sellers can also realize of this and cancel the commissions. The greedier the criminals are, the easier the seller will notice," he says. "However, if the criminal is smart enough they can be doing this for years without anyone noticing it, and 'earning' thousands each month."

eBay has been aggressively going after cookie-stuffers, and a Las Vegas man was arrested in February for allegedly running a cookie-stuffing operation where he sold a cookie-stuffing tool that let fraudsters siphon advertising referrals or commissions out of eBay, according to a [published report](#) in *Wired*. eBay was duped into paying these referrals "despite the fact that no eBay advertisement or link on the affiliate website or webpage had actually been clicked," according to the charges.

Kyle Adams, chief architect at Mykonos, says it makes sense that the Mariposa operators didn't include cookie-stuffing because it would be too conspicuous to execute this type of web fraud via a botnet. "You don't need to compromise a machine to be doing it. It can be launched by posting a comment," Adams says. "For a bot, it would be overkill. There are easier ways to do it, and a botnet would be visible."

Adams says maybe the bot software creator for Mariposa just offered the feature to see if it would fly. "He might have been throwing it in to see if people pick it up," he says.

Al Huizenga, director of product management at Mykonos, says it's the websites who join big affiliate programs for the Amazons and eBays, for instance, that are getting hurt. "They're not going to get paid out. It's not their fault ... they've been exploited. But it pollutes all the downstream transactions as a result of that behavior," he says. "But the eBays who get the final traffic continue to do quite well."

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

Care to Comment?

Subject (max length: 75):

Comment:



Vulnerability Management Newsfeed

- [Sourcefire Announces Next Generation Firewall](#)
- [WatchGuard Ships Next-Generation Firewall For Enterprises](#)
- [Former Iron Mountain Chief Bob Brennan Becomes CEO Of Veracode](#)
- [Free Security Tools From Qualys To Prevent Online Holiday Scams](#)
- [BEAST Browser Security Threat Is Not As Fierce As It Looks. Says Context Information Security](#)
- [Rapid7 Secures \\$50 Million In Series C Funding](#)

[MORE NEWSFEED >>>](#)

Tech Centers

- Advanced Threats
- Authentication
- Cloud Security
- Compliance
- Database Security
- Insider Threat
- Mobile Security
- Security Monitoring
- Security Services
- SMB Security
- Vulnerability Management