Cybercrooks Trick Gawker Into Serving Malware-Laced Ad

By Kevin Poulsen ✉ October 27, 2009 | 2:25 pm | Categories: Miscellaneous

Remember when the global economic crisis was supposed to drive legions of desperate, unemployed computer programmers into cybercrime? It turns out the real threat comes from unemployed advertising agents.

Scammers posing as the well-known ad agency Spark-SMG tricked Gawker Media into running a fake Suzuki ad last week that served malicious code, according to a report in Silicon Alley Insider. A similar scam hit the *New York Times* in September. Unlike the newspaper, Gawker has released the e-mails it exchanged with the scammers, and the messages show just how confidently the perps navigated the ad-buy process.

"We are only interested in standard IAB banner sizes right now as that's what we have sign off for," wrote fake person George Delarosa, at one point in the negotiations. "Please whip up a proposal and let's try and get a rush on getting something going as we are in need of some major imps by the end of the month as we are under-delivering on our monthly impression levels for September."

I'd rather voluntarily install the malware then read that paragraph again. But it does show that the scamsters — who are probably behind the *Times* attack as well — know exactly what they're doing. In addition to the authentic prose, the crooks backed their play with a working phone number in a Chicago area code, where the

real Spark is based, and a copycat domain name.

"Whoever it is definitely worked in online ad sales at some point ," an anonymous Gawker salesperson wrote the Insider.

With legitimate ad sales in a slump industrywide, malware-laced banners and, more commonly, just plain deceptive ads are enjoying way too much access to legitimate outlets these days, sometimes delivered through third-party ad networks, and sometimes through direct sales like in the Gawker and *Times* attacks.

The problem has grown so large that New York ad company Epic Advertising has hired a former FBI cybercrime agent to head a division that scrutinizes potential advertisers. The company is hoping to distinguish itself in the market with a commitment not to run malware, dubious testimonials and ads linking to fake news articles.

"All ads are previewed in advance with the sales team, then they have to go through Compliance to make sure they don't say anything funky," says Epic's E.J. Hilbert, who worked against Eastern European cybercrooks while in the Bureau. "We are the watchdogs and the hound dogs. I think like a bad guy. I think like a guy who's going to manipulate these situations, and help to devise a way to make sure that we don't fall for it."

For those without G-men on staff, a few minutes of sleuthing might prevent gaffes like Gawker's. While Gawker's salesperson says the company did all it could to scrutinize the fake Suzuki ad, a quick phone call to a known and trusted number for the real Spark would likely have put the kibosh on the attack before it began.

The ad ran for "less than 5 days last week," said Gawker's James Del, in an e-mail to Threat Level. "This was a very malicious piece of code that seemingly took advantage of unpatched Adobe software, though we don't have details on how exactly that worked. It was not a 'trick' ad, wherein users were prompted to install something … It simply strong armed it's way through a vulnerability and infected the computer.

"This isn't a worm that goes unnoticed,' Del added. "It would have crippled the user's computer in a few moments, based on the reports we received. There would have been pop ups, freezing, and multiple file downloads taking place."

—

Updated 16:35 with Gawker's response.

See Also:

- *New York Times* Reforms Online Ad Sales After Malware Scam
- This Just In: Fake News Sites Are Great!

Post Comment | Permalink

Comments (8)

Posted by: vulturetx | 10/27/09 | 5:05 pm |

was it a real phone and web site even –
or was it just a google voice with a 612 # and google hosted domain with a homonym url linked to a phony account? As for web marketing speak, they could have picked it up anywhere, even at a Disney convention.

Posted by: zanozimek | 10/27/09 | 5:22 pm |

There's nothing authentic about their "marketing-speak"; the cited example is so bizarrely forced it's hilarious. Which is unfortunate as the notion of a renegade ad-man striking back at the parasitic nature of that industry is romantic, in a way.

Posted by: technophile | 10/28/09 | 12:03 am |

You know what I just did? Install Ad Block Plus. By being so careless they are only hurting their bottom line.

Posted by: sub1ime14 | 10/28/09 | 3:58 pm |

Precisely why I use a HOSTS file to redirect all DNS lookups for these ad agencies back to the localhost. "The page cannot be displayed" truly has a good feeling now.

Posted by: fityxxpayeevkl | 10/28/09 | 5:03 pm |

The fact that the anonymous "Salesperson" at Gawker thinks that you have to had worked in ad ops to write like that just shows how grossly idiotic so many people in ad ops are.

Posted by: alex1234 | 11/2/09 | 6:51 am |

The jeweler's famous name and Fifth Avenue address are very popular and important for the fans. tiffany jewellery online shop sells varieties of tiffany jewelry products, including tiffany bracelet, tiffany necklace, tiffany ring, tiffany earrings, tiffany pendant and various other tiffany replica jewelries. We are one of the biggest suppliers of tiffany jewelry sale company in the globe.A gleaming Passport Cover in colorful patent and textured leather opens the way to adventure; and a sterling silver key ring engraved with 'Class of 09' opens the door of a first home.

Louis Vuitton Matsuya Ginza Store done renewal and displays their "speedy" archives over past years tiffany jewellery online shop sells varieties of tiffany jewelry products, including tiffany bracelet, tiffany necklace, tiffany ring, tiffany earrings, tiffany pendant and various other tiffany replica jewelries. We are one of the biggest suppliers of tiffany jewellery sale
,Louis Vuitton has been welcomed by many louis vitton handbag lovers. I think there is no cheaper louis vuitton handbags than you in the world. "speedy" is known as Louis Vuitton's iconic line. Every arranged bags were very interesting.

Posted by: cindy3 | 11/13/09 | 3:18 am |

Everyone has many accessories whether men or women. Tiffany's jewelry have become an indispensable part in people's lives, many people like tiffany ring , tiffany earrings and so on. Tiffany jewelry is so luxurious and attractive. There are a lot of products,
tiffany earrings necelaces and bracelets. I perfer totiffany charms. Each one is very delicate and original. They let people feel that the products are given more care to make and as people see the products, they desire to own one. When I have money, I will buy one for myself.tiffany sets

---

Posted by: mr4t22 | 05/12/10 | 10:42 pm |

müzik dinle
şarkı dinle
sikiş izle
müzik dinle
video izle
