Security researchers in force at USENIX Security

August 10 2012

At USENIX Security 2011, UC San Diego computer science faculty, staff, students and alumni were out in force. They expect a similar turnout for the 2012 symposium, which runs Aug. 8-10, and will feature four papers authored or co-authored by CSE researchers (the same number as in 2011).

Everybody who's anybody in the no-longer-arcane field of computer security is out in force in Bellevue, Wash., this week at the 21st USENIX Security Symposium, the leading computer systems and networking security conference. Before the official kickoff Aug. 8, Computer Science and Engineering Ph.D. student Feng Lu presented a joint paper with fellow graduate student Jiaqi Zhang and CSE professor Stefan Savage at the 7th USENIX Workshop on Hot Topics in Security (HotSec '12) on Tuesday. Their paper, "When Good Services Go Wild: Reassembling Web Services for Unintended Purposes," is the subject of a report in MIT Technology Review about 'a menacing Facebook-

Google mashup'.

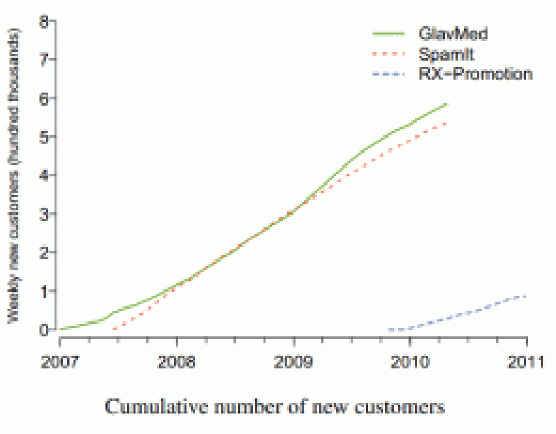
For the second year in a row, researchers from the Department of Computer Science and Engineering are authors or co-authors on four papers accepted to the main USENIX Security meeting. These include Prof. Sorin Lerner's work on browser security presented Aug. 8, and postdoc Nadia Heninger's Aug. 9.

Before that, the conference opened Wednesday with a kickoff session on "Spam and Drugs." A team including Professors Stefan Savage and Geoffrey Voelker, research scientist Kirill Levchenko, and others, stirred interest with their paper on "PharmaLeaks: Understanding the Business of OnlinesPharmaceutical Affiliate Programs." Former postdoc Damon McCoy (now a professor at George Mason University) made the presentation co-authored with the UC San Diego team as well as collaborators at the International Computer Science Institute and private security expert Brian Krebs.

While technically a co-author on the PharmaLeaks paper, Krebs says his participation primarily involved the donation of major rogue pharmaceutical affiliate databases that "had fallen into [his] lap" while he was reporting on the turf war between the Russian businessmen behind Rx-Promotion and sister programs SpamIt and GlavMed, some of the biggest spam-based marketing companies in the world. Krebs recently previewed the PharmaLeaks paper and gave us permission to republish the story that follows from his widely-followed blog, Krebs on Security:

PharmaLeaks: Rogue Pharmacy Economics 101

Consumer demand for cheap prescription drugs sold through spam-advertised Web sites shows no sign of abating, according to a new analysis of bookkeeping records maintained by three of the world's largest rogue pharmacy operations.



Growth in new customers until GlavMed and SpamIt went under in 2010, but rival RX-Promotion (all based in Russia) is steadily gaining ground.

Researchers at UC San Diego, the International Computer Science Institute and George Mason University examined caches of data tracking the day-to-day finances of GlavMed, SpamIt, and Rx-Promotion, shadowy affiliate programs that over a four-year period processed more than $170 million worth of orders from customers seeking cheaper, more accessible and more discretely available drugs. The result is perhaps the most detailed analysis yet of the business case for the malicious software and spam epidemics that persist to this day.

Their conclusion? Spam — and all of its attendant ills — will remain a prevalent and pestilent problem because consumer demand for the products most frequently advertised through junk email remains constant.

“The market for spam-advertised drugs is not even close to being saturated,” said Stefan Savage, a lead researcher in the study, due to be presented at the 21st USENIX security conference. “The number of new customers these programs got each day explains why people spam: Because sending spam to everyone on the planet gets you new customers on an ongoing basis, so it’s not going away.”

The researchers found that repeat customers are critical to making any rogue pharmacy business profitable. Repeat orders constituted 27% and 38% of average program revenue for GlavMed and SpamIt, respectively; for Rx-Promotion, revenue from repeat orders was between 9% and 23% of overall revenue.

“This says a number of things, and one is that a lot of people who bought from these programs were satisfied,” Savage said. “Maybe the drugs they bought had a great placebo effect, but my guess is these are satisfied customers and they came back because of that.”

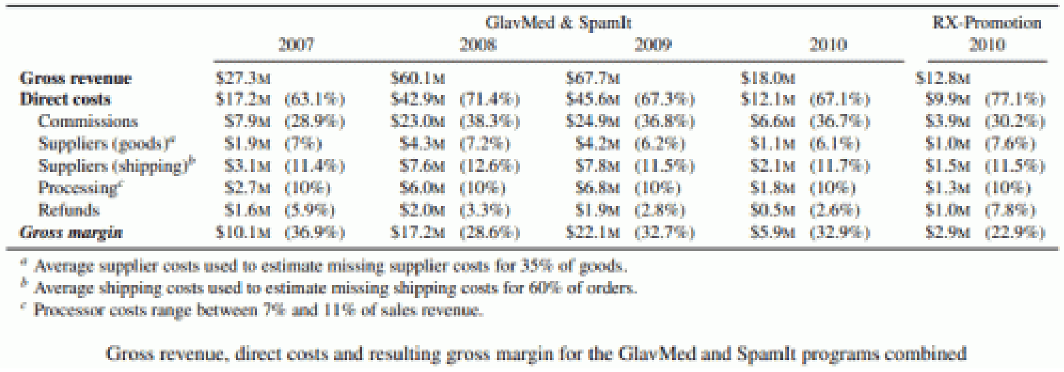
Whether the placebo effect is something that often applies with the consumption of erectile dysfunction drugs is not covered in this research paper, but ED drugs were by far the largest category of pills ordered by customers of all three pharmacy programs.

One interesting pattern that trickled out of the Rx-Promotion data underscores what made this pharmacy affiliate unique and popular among repeat buyers: A major portion of its revenues was generated through the sale of drugs that have a high potential for abuse and are thus tightly controlled in the United States, including opiates and painkillers like Oxycodone, Hydrocodone, and mental health pills such as Adderall and Ritalin. The researchers noticed that although pills in this class of drugs — known as Schedule II in U.S. drug control parlance — comprised just 14 percent of orders for Rx-Promotion, they accounted for nearly a third of program revenue, with the Schedule II opiates accounting for a quarter of revenue.

“The fact that such drugs are over-represented in repeat orders as well (roughly 50 percent more prevalent in both Rx-Promotion and, for drugs like Soma and Tramadol, in SpamIt) reinforces the hypothesis that abuse may be a substantial driver for this component of demand,” the researchers wrote.

The ‘Partnerka’ Economy

The study also seeks to explain the revenue model behind these pharmacy affiliate partnerships — often referred to in Russian as “partnerkas.” In a typical partnerka, the program sponsors handle everything from purchasing pill-site domains and arranging hosting, to procuring the pills, credit card processing, managing shipment and customer support. The sole role of the affiliates or spammers is to undertake the somewhat riskier job of figuring out ways to drive tons of traffic to the pill sites.



	GlavMed & SpamIt				RX-Promotion
	2007	2008	2009	2010	2010
Gross revenue	$27.3M	$60.1M	$67.7M	$18.0M	$12.8M
Direct costs	$17.2M (63.1%)	$42.9M (71.4%)	$45.6M (67.3%)	$12.1M (67.1%)	$9.9M (77.1%)
Commissions	$7.9M (28.9%)	$23.0M (38.3%)	$24.9M (36.8%)	$6.6M (36.7%)	$3.9M (30.2%)
Suppliers (goods)[a]	$1.9M (7%)	$4.3M (7.2%)	$4.2M (6.2%)	$1.1M (6.1%)	$1.0M (7.6%)
Suppliers (shipping)[b]	$3.1M (11.4%)	$7.6M (12.6%)	$7.8M (11.5%)	$2.1M (11.7%)	$1.5M (11.5%)
Processing[c]	$2.7M (10%)	$6.0M (10%)	$6.8M (10%)	$1.8M (10%)	$1.3M (10%)
Refunds	$1.6M (5.9%)	$2.0M (3.3%)	$1.9M (2.8%)	$0.5M (2.6%)	$1.0M (7.8%)
Gross margin	$10.1M (36.9%)	$17.2M (28.6%)	$22.1M (32.7%)	$5.9M (32.9%)	$2.9M (22.9%)

[a] Average supplier costs used to estimate missing supplier costs for 35% of goods.
[b] Average shipping costs used to estimate missing shipping costs for 60% of orders.
[c] Processor costs range between 7% and 11% of sales revenue.

Gross revenue, direct costs and resulting gross margin for the GlavMed and SpamIt programs combined

Key economic indicators for the combined programs of sister companies GlavMed and SpamIt for 2007-10 and for newcomer Rx-Promotion for 2010 only.

And for this, the affiliates are rewarded handsomely. The researchers observed that affiliate commissions ate up between 30 to 40 % of revenue for all three programs. Interestingly, the researchers found that while each program employed hundreds of affiliates, most of the affiliates earned next to nothing. Rather, just 10% of the highest-earning affiliates accounted for 75-90% of total program revenue across the three affiliate programs.

“This is the brilliance of the affiliate program model, because you let every schmuck come in and try to do their thing, and you don’t care whether they succeed because you pay them only on a commission basis,” Savage said. “So all affiliate programs want to get the good affiliates, but the problem is they may not know who’s good ahead of time, so you let lots of people in, but most of the affiliates are just wasting their time.”

Nearly all of the top earners for SpamIt and Rx-Promotion are the affiliates thought to be responsible for running the world’s largest spam botnets, including Cutwail, Rustock, Waledac, Mega-D, Srizbi, and Grum.

So how much did the affiliate program sponsors themselves make? After paying affiliates (30-40%), suppliers (~7% of gross revenue), for shipping (a loss leader, it turns out, at between 11% and 12%), credit card processing (10%) and a host of other direct and indirect costs, the sponsors made a net profit of about 20% of gross revenue.

“Clearly these affiliate programs are profitable, but they are operating a business enterprise,” the researchers wrote. “Their profit is still only a fraction of the overall revenue.”

While the overall volume of email that is spam recently fell to historic lows, that ratio been steadily creeping back up since April, according to Symantec. It will be interesting to see if this trend continues as other affiliate programs compete to meet customer demand and lay claim to the market shares once held by the likes of GlavMed, Rx-Promotion and SpamIt.

Provided by University of California - San Diego

Citation: Security researchers in force at USENIX Security (2012, August 10) retrieved 17 July 2024 from https://phys.org/news/2012-08-usenix.html