digitalcitizens alliance

DIGITAL CITIZENS ALLIANCE REPORT

THE TANGLED WEB: HOW ONLINE CRIME SYNDICATES WORK TOGETHER TO CHEAT, STEAL, AND LIE ONLINE

TABLE OF CONTENTS

UNDERSTANDING ONLINE CRIME SYNDICATES

Rogue Internet pharmacies and spam. Software, music and movie piracy. Stolen corporate secrets and online extortion attacks. The wages of cybercrime are extracted from nearly every corner of the Internet, with legitimate businesses and major producers of intellectual property absorbing the costs of some of the biggest shakedowns.

But shrinking the profits of pirates and cybercriminals involves following the money and finding creative ways to disrupt this flow of crooked capital. Success on that front demands an understanding of how the underground operates and where the pressure points reside. This paper will examine the key pillars that support most criminal commerce online today, including black market online bazaars, cybercrime joint ventures, and underground exchanges. We'll also spotlight recent examples in which rights holders were able to undermine a cybercrime ecosystem simply by disrupting one or more of these key criminal components, using established reporting methods with the major payment card networks.

THE PIVOTAL ROLE OF 'PARTNERKAS'

Cybercrime is often misunderstood as illegal activity carried out by organized and highly skilled gangs. Yet the evidence to date suggests that most computer crime is perpetrated by a loose confederation of independent contractors who work together when needed -- but only when it is mutually beneficial to all cooperating parties.

When independent cybercriminals combine their skills and efforts, it usually takes place in one or both of two environments: The cybercrime forum, and

the affiliate program, also known as the "partnerka". Both forums and partnerkas allow independent actors to pool their resources in ways that may serve a greater good (or, in this case, ill) but which ultimately are aimed at creating personal wealth, power and greater access to the tools that may further future online criminal schemes.

As events over the past two years have shown, tackling Internet piracy and intellectual property crime requires weakening the glue that binds these communities together. And that means undermining trust relationships between cybercriminals, isolating and apprehending key members, and making it more difficult for them to receive payment for their crimes. This paper will focus on that last -- and most effective -- strategy: **Following the money**.

DIVERSIFICATION

For a great many denizens of the cybercrime underground, it is not enough to be involved in one shady operation. Some of the most successful miscreants are those who diversify their operations. Your average crime forum member has ties to multiple types of illegal or illicit online enterprises. The reason for this is simple: If one moneymaking scheme fails to generate an income, the miscreant can then direct his efforts and attention to another program.

Most forums feature a myriad of services for driving traffic to affiliate programs that pimp a variety of products. These include rogue pharmacy sites, fake

antivirus or ransomware affiliate programs, counterfeit software and prescription drugs, as well as organized dating and reshipping scams, toll fraud and SMS billing schemes.

The affiliate model online is rooted in the adult content industry at the turn of the millennium. At that time, pioneers in the online credit card processing industry were among the first to employ it on a large scale to sell subscriptions for porn sites. Many of the tactics used to drive potential customers to these affiliate porn sites -- search results manipulation, click redirection, mousetrapping, and browser hijacking -- were soon adopted by affiliate programs that rose up to help peddle fake AV, phony pills and the sale of pirated software.

The reason that it is common for miscreants to engage in multiple forms of seemingly unrelated online fraud is that most of these money-making schemes are modular, or "plug-and-play," if you will. The people running the affiliate operation, known as the "sponsors," handle nearly every aspect of the business, including credit card processing and customer support, to creating the content or procuring the "product" for sale. Whether the product is counterfeit prescription drugs, knockoff handbags, rogue antivirus software, pirated software or phantom Russian brides, the affiliate's singular role is the same: To drive willing or unwitting clients or "traffic" to the program's Websites.

This dynamic of affiliate programs allows the sponsors to (in theory, at least) maintain a safe distance from the more illicit aspects of the business -- which typically employ the use of hacked PCs by the thousands. The affiliates benefit from the arrangement by being able to quickly unplug their traffic from one affiliate program in favor of another that may offer more attractive

terms, such as higher commissions, more immediate and predictable paydays, better customer service and product selection.

The motivating factor for the affiliate is that these programs are pay-per-acquisition; the affiliate only gets paid when a new "customer" or victim is enticed, tricked or cajoled into shelling out money for the service or good in question. In short, the sponsors don't need to worry about the latest and greatest methods for finding new customers; they leave that to the affiliates, who are continually incentivized to devise new and ingenious ways to gin up sales.

With nearly all of these affiliate programs, the customer conversion ratios are sometimes infinitesimal, (usually less than one to three percent). As a result, if the affiliate wants to make any serious money, he needs to drive huge volumes of traffic to the program's resources on a near-constant basis. Traditionally, the most popular methods of driving traffic to affiliate programs have involved compromising Websites, hacking PCs, spamming, or some combination of these methods.

TRAFFICKING IN TRAFFIC

The easiest and cheapest way to drive huge volumes of traffic online is to purchase this traffic from traffic vendors (known as "traffers"). But this gets expensive over time. For most miscreants, it makes more sense long-term to build a botnet, or a collection of hacked PCs that the miscreant can control from afar for a variety of activities. Yet, even miscreants who operate botnets will need to buy traffic and/or "installs" of their bot malware on other bot networks. Most botnets require constant care and feeding, necessitating the continued infection of new PCs as older bot systems get cleaned up by antivirus tools or taken offline by their owners.

The botmaster can use computers in his network to relay junk email advertising whatever service, product or scam is being pushed by the affiliate program(s) to which he's subscribed. If the botmaster is a member of a rogue antivirus or ransomware affiliate program, he can seed all of the infected PCs in his botnet with an installer program that warns the system's legitimate owner that the computer will be held for ransom unless and until the victim pays up (or hires someone to disinfect the PC!)

Not all miscreants who wish to join cybercrime affiliate programs have botnets at their disposal, nor indeed do they have access to all of the resources one needs to build and maintain a functional and profitable botnet. Fortunately for these users (and for the underground criminal ecosystem as a whole, as we shall see), there are dozens of underground forums that sell every manner of turnkey solution that can enable a would-be fraudster to get their very own cybercrime operation up and running very quickly -- for a price.


http://

FRAUD FORUM ENVIRONMENT

There are literally dozens of underground fraud forums catering to a dizzying range of nationalities, specializations and interests. Some forums let new users register without any special qualifications, but most forums operate on a reputation basis, meaning new users must be vouched for by an existing member or several members. In addition, the applicant may need to pay a nonrefundable registration or entry fee. In the more exclusive forums, new applicants are repeatedly questioned by more established members of the community -- a period in which the applicant is quizzed about his past projects and encouraged to prove that he is a "legitimate" computer crook and deserving of membership. Ultimately, the applicant's acceptance to or rejection from the forum may hinge on the tally of votes cast by existing forum members. This voting mechanism is more common on smaller, more exclusive crime forums.

A forum member's status, influence and privileges are directly tied to his "rep," or the reputation points awarded or subtracted by other members. Longtime members accumulate rep points that they may hand out to other members, usually in recognition of a deal that was consummated in a manner that was acceptable to both parties of the transaction (much like eBay users rate transactions by leaving positive or negative "feedback" points). In this way, members who routinely abuse, mistreat or rip off other members are quickly shunned. Depending on the nature of the infraction and against whom it was committed, the offending member may be placed on probation (knocked down to "deer" status), or summarily exiled from the forum.

The most shameful rank on any crime forum is "ripper," which warns other members against transacting with that person. This status is generally assigned by forum administrators after sufficient proof is provided (instant message chat logs, e.g.) that the alleged ripper was paid for goods or services that he did not

render. Members assigned to ripper status are often given an opportunity to right the alleged wrong; those who refuse to address the complaint are usually banned from the forum.

These crime forums exist because they generate a steady stream of income and raw resources for the forum owners and operators. Many fraudsters will only transact with other fraudsters if the forum offers an escrow service. This is a security mechanism in which the money for a given transaction is held by the forum administrators until both parties signify that the transaction was completed satisfactorily. For this, the forum administrators take a small percentage of the escrow amount, not unlike a gambling den that takes a rake from all players for hosting the game.

It is tempting to conclude that crime forums waste time and resources inviting and accepting novice hackers, many of whom end up being rippers. However, on reasonably sized fraud forums (1,000 or more members), a majority of the money flowing through the forum will come from relatively novice hackers paying established "verified" vendors for turnkey services of one form or another. Verified vendors pay annual fees (sometimes thousands of dollars) to have this verified label, which acts as a sort of seal of approval and trustworthiness that lets potential customers know these members have been vetted. Thus, novice members are tolerated because they provide a steady stream of income for the forum administrators and top verified vendors.

The services for sale on a forum are quite stratified, divided up into sub-forums of various specialities. For example, a typical fraud forum will have a subforum dedicated to spam, another reserved for those interested in or transacting in services aimed at laundering money. Yet another strata of the forum will serve as

a home base for affiliate programs, and so on.

If one looks at enough of these forums, it is common to see the same personas as moderators in their speciality area across multiple online communities. Why is that? One explanation is that these individuals have achieved such a level of proficiency in what they do that they know nearly everyone of consequence in their field, and consequently have tremendous access to resources in their area of specialization.

One high-profile miscreant who typifies this dynamic is a well-known spammer who uses the nickname Peter Severa. He is better known on several crime forums as simply "Severa," and is believed to be responsible for the Waledac and Storm spam botnets, among others. Both Spamhaus and KrebsOnSecurity.com blogger Brian Krebs have presented evidence that Severa's real name is Peter Levashov, and that he is a resident of St. Petersburg, Russia.

Severa was the moderator of the spam services subforum on Spamdot.biz, a shadowy underground forum that catered specifically to individuals engaged in pharmacy spam affiliate programs. He also moderates the spam subsections on multiple other Russian hacking forums, including zloy.bz, pustota.tw (until recently, the new spamdot) and lampeduza.net, and manages fake antivirus affiliate programs.

Severa is a textbook example of a key figure in the underground who acts as a kind of "force multiplier" -- a miscreant who operates across horizontal and vertical cybercrime markets and provides a kind of social glue for the underground economy. Spam, for example, is a method of spreading digital disease, be it counterfeit software, fake antiviruses or links to rogue pharmacy operations. As

a result, miscreants who provide a broad array of spamming services necessarily are linchpins in the cybercrime economy, with a diverse set of contacts and connections throughout the Underweb.

FOLLOWING THE MONEY

For organizations interested in making it more difficult and costly for these criminal enterprises to operate, it makes much more sense to focus attention on pressuring and isolating the merchant banks that are servicing these industries.

To that end, it is instructive to consider the work already done by a team of researchers from the International Computer Science Institute, George Mason University and the University of California, San Diego. In 2010, the group began making targeted "test buys" at Websites run by a variety of affiliate programs pushing cheap pills, purses and counterfeit software. As Krebs writes:

"The test buys were intended to reveal relationships between the shadowy merchants and the banks that process credit and debit card transactions for these businesses. Following the money trail showed that a majority of the purchases were processed by just 12 banks in a handful of countries, including Azerbaijan, China, Georgia, Latvia, and Mauritius."

Contracts between the banks and Visa and MasterCard stipulate that merchants are prohibited from selling goods and services that are illegal in the country into which those goods or services are being sold. The credit card associations have a standard process for accepting complaints about such transactions, in which they warn the online merchant's bank (including a notice of potential fines

for noncompliance). After a complaint about such activity, the merchant's bank conducts its investigation and may choose to contest the issue if they believe it is in error. But if the bank decides not to challenge the complaint, then they will need to take action to prevent future such transactions, or else face an escalating series of fines from the card associations.

The researchers said they submitted the test buy results to a database run by the International AntiCounterfeiting Coalition (IACC), a Washington, D.C.-based non-profit organization devoted to combating product counterfeiting and piracy.

The team noticed that in case after case, merchant accounts that were used in fraudulent activity for some extended period of time before they filed a complaint with the IACC generally stopped being used within one month after a complaint was lodged.

In May 2011, Visa initiated a new program, the so-called "Global Brand Protection Program". How this would turn out for banks and merchants no one knew at the time, but a lengthy thread posted to one popular pharmacy affiliate forum explained why so many rogue pharma programs were being hit with fines, and much of it was because of the reporting the researchers made about their test buys to the IACC.

The rogue pharma program manager lamented: "After several months, Visa begins to act, and beginning in November 2011, fines of $25,000 USD on every domain containing brands Viagra, Cialis and/or Levitra or other copyrighted medications began raining down on merchants."

The researchers were conducting their test buys at the same time the U.S.

Congress was debating highly controversial proposals to expand the powers of law enforcement to more aggressively pursue software and brand piracy. The proposals, known as the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA), were met with stiff opposition from privacy rights and Internet freedom groups.

Some brand holders, including factions representing the movie, music and pharmaceutical industries, argued that the new laws were needed to crack down on the rampant abuse and theft of corporate trademarks and copyrighted digital media. Critics of the bills said they would stifle free speech, violate user privacy, and kill jobs. Both measures were ultimately abandoned, in large part due to an overwhelming public outcry against them.

Remarkably, the academic researchers proved that brand holders already have the authority and powers to hit scammers, spammers and content thieves where it counts the most: In their pocketbooks.

"It doesn't require a judge, a law-enforcement officer or even much in the way of sophisticated security capabilities. If you can purchase a product, then there's a record of it and that record points back to the merchant account getting the money," said Stefan Savage, a professor of computer science at UCSD and one of the principal authors of the study. "Visa and MasterCard frown on sales of illegal purchases made on their networks and will act appropriately on complaints from brandholders based on undercover purchases."

Savage said it doesn't take concerted action by all of the affected brands to have a major impact on the rogue businesses that incentivize this type of commerce. On the contrary, he said one software brand holder pursued the merchant banks

tied to all of the group's test buys for its products with such ferocity and swiftness that it virtually shut down the market for pirated brand name software [a.k.a "OEM"] overnight.

"This vendor went after everything. They did it so quickly — and not only for their own products — that it all but shut down the entire OEM ecosystem," Savage said. "A couple of [OEM affiliate programs] survived by getting rid of that company's brand, but in the beginning, when people had no clue what's going on, it shut down the entire business for everyone."

Government regulation frequently over reaches or misses the mark entirely, raising costs for industry and introducing unintended consequences for third-party market participants. Those seeking new laws to combat cybercrime and piracy should look to the example set by the UCSD researchers. Their actions and results prove that rights holders already possess remarkably effective and fast-acting tools for enforcing trademark and copyright law violations online.

www.digitalcitizensalliance.org