Viruses, Phishing, and Trojans For Profit

Kelly Martin,

Following the 2006 International Virus Bulletin Conference, Kelly Martin takes a look at the profit motives of the cyber criminals behind modern viruses, targeted trojans, phishing scams and botnet attacks that are stealing millions from organizations and individuals.

Virus Bulletin 2006, the international virus conference, was held in Montreal this year. Just a few weeks ago I was fortunate enough to attend many of the presentations, which ranged from topics of targeted trojan attacks, botnets and new methods of botnet coordination, to the growing criminal element behind viruses. It's sometimes shocking to see how much the virus world has changed in the last few years. I'd wager that if there was just one overall theme of the conference, it was about criminals and the new profit motive behind today's malware. Long gone are the days when viruses were made by hackers just for fun.

My favorite quote taken from the excellent, low-key conference was during a panel discussion on fighting cyber crime: "If anyone in the audience is a member of organized crime, please raise your hand." *[laughter]*

There's big money on the criminal side of viruses these days. The past two or three years has seen a dramatic rise in for-profit virus activity at every level, from the people running botnets and making money off spyware to widespread phishing attacks and various trojans that encrypt a user's data and request a ransom. There are countless viruses that are used to send out a very large amount of spam, which is quite profitable. There's money laundering and organized crime involved, because the dollar amounts are becoming huge. And then there's the whole range of aggregate identity and credit card theft plus the targeted trojans that can be used to steal millions of dollars from just one company. Money, money, and viruses. The situation is getting pretty grave, indeed.

I'd like to look at the profit motive in some detail, to understand this dangerous new trend. First allow me to lump together the myriad of today's for-profit virus threats into just two camps, for the purpose of this column: those threats that target the Little Guy, like individuals and individual organizations (via targeted trojans, general trojans, rootkits and targeted hacking), and those amalgamated threats that target Big Populations (via botnets, tonnes of spam, and spyware). The virus folks behind both camps seek to steal money, information and identities. But they work in different ways.

Scammers and spammers work on the aggregate

Attacks against Big Populations tend to skim a little bit of money off many people. A teenager or young adult controlling a botnet can make a six figure income, from between just a few hundred dollars to many thousands of dollars each month. They install spyware on the infected machines in the botnet, and sleazy spyware companies pay them real money for it. They also sell access to the botnet for spamming, and they make money from this by the hour. They can also point their botnet at a casino, poker, or porn website and extort money from the owners by threatening to issue a Distributed Denial-of-Service attack, which would take the company offline. Or, they can just log everything on the thousands (or hundreds of thousands, or even millions) of machines in a typical botnet, aggregate the logs up and sell them by the megabyte. Inside those logs might be credit card numbers, online banking passwords, Social Security Numbers, and much more. Many botnet owners don't yet focus on this, as they are more interested in stealing a little bit away from everyone.

I think it's fair to say that the criminals running botnets, until a few years ago, didn't realize the kind of power they had. I'd argue that they still don't, as there is a treasure trove of information on each machine that is not being mined to its fullest. But the day

is coming.

Phishing fraud in aggregate

Phishing fraud has also proven itself to be enormously profitable in aggregate. In just a few years, "phishing" has become a household name for stealing banking details from hapless victims over the Internet. There's a sucker born every minute, and they all use e-mail nowadays – thanks to our woefully insecure e-mail system, people get lured to a fake site. What might be surprising is how quickly a phisher can turn a profit and convert that "virtual money" into real cash.

At Virus Bulletin this year, Guillaume Lovet from Fortinet gave an interesting presentation about "dirty money on the wires: the business models of cyber criminals" where he detailed the often complex set of arrangements behind the Big Population risk. His accompanying paper was published in the Proceedings of the 16th Virus Bulletin International Conference.

From younger workers doing technical grunt work to older folks doing the money laundering and interacting with organized crime, the illicit business model runs the full gamut of criminal activity. Most interesting to me was Lovet's discussion of the intense profitability around phishing – after he presented a typical phishing business model, he compared its profitability to the manufacture and sale of heroin. More incredibly, he argued that electronic phishing scams might just be even more profitable than selling drugs. The exact numbers and the drug analogy can be disputed, of course. But based on the short time needed and the large payoff I'd say there's probably less risk of getting caught doing phishing (as opposed to selling drugs) as well. Lovet found that a typical phishing profit might range from $2,500 to $25,000 - not bad for a day's work.

Looking at the groups behind the theft gives a keen insight to the business of cyber crime. Low risk, high profit, and it's unlikely that the criminals will get caught. No wonder phishing has exploded in just a few years. More than that, it's unlikely that the victims will even know something was wrong with their Windows computer until their identity, banking or credit card details are compromised and used. That $499 PC purchased mail-order for your Aunt isn't looking so attractive anymore, is it?

That's pretty much where we are today. The only problem with Lovet's analysis, as I could see, is around getting hard numbers and actual case studies – but understand that the very nature of the crime means that this sort of data is likely only held by the FBI, Interpol and other national police agencies. And for every crime ring they crack, there are countless more that go unpunished.

Big money from the Little Guy

It's pretty common to find viruses or trojans now that encrypt a user's hard drive and then demand a ransom to give the data back. This is a somewhat targeted attack focusing on individuals, the Little Guy, and is small potatoes for the most part (unless you're one of the victims). Where it gets interesting is with the upturn in targeted trojans that seek out individual companies and then try one do one thing very, very well.

Targeted trojan attacks are just as one might expect: software that is very focused on stealing from individual companies in a stealthy manner. The people behind these trojans are criminal hackers going after some very specific types of data from within just one target: a large bank, a military installation, a Fortune 500 company or a government office. They craft a customized trojan horse – or purchase one – that avoids detection from anti-virus software. Then they try to lure at least one person from the target organization to install it, and voila. Reconnaissance begins. The trojan could be sent via e-mail, but that seems unlikely because it's so obvious. Even accounting people today know not to click on unknown attachments in e-mail. But what about a blended attack, a malicious Word or Excel document sent in e-mail with a zero-day exploit? Or it could

be as simple as sending the victim a link to a web page with a zero-day exploit for Internet Explorer, easily infecting the machine and prompting the download and installation of a malicious trojan. Step one is complete.

These are threats that are very difficult to detect, because by their nature they almost always avoid the signature-based detection models used by anti-virus software – no signature will have been created yet because none of the AV companies would have seen this exact trojan signature before. Some types of heuristics in various AV software can still identity unknown trojans, but the results are not always consistent or reliable. The point of this discussion is that sometimes the Little Guy, the individual or isolated company, is not so little after all.

Customized trojans, for a price

If there's one thing we've learned, just about anything is available for a price.

Dmitri Alperovitch from CipherTrust gave an excellent presentation at Virus Bulletin on "phishing trojan creation toolkits." His talk was about how it's now possible to go out and *purchase* a fully customized Trojan horse for phishing purposes, one that can inject new fields into a legitimate web page. In other words, the average Joe Criminal can go out and purchase a toolkit that can create a targeted, fully customized trojan horse capable of evading the detection of anti-virus software, and then use it to steal money from innocent people. There's still the issue of getting this trojan in the right place, but let's take this one step at a time.

The example Alperovitch showed was quite advanced, capable of numerous features like support for encryption and two-factor authentication that allows a less sophisticated cyber criminal to make just the right kind of trojan. Setup the required features and click the button that says compile. I found it all quite shocking, to be honest - I did not know how far these trojan toolkits have come, or how much it can lower the bar. One of the greatest security fears of any organization is (or should be) targeted trojans, because of their capability to steal virtually any information inside an organization and remain undetected for some time. I *won't* take the liberty of mentioning some of the toolkits here, which range from $100 to $5500.

What can these trojans help steal? Money, for starters. Phishing works because most people can't identify a fake website. Let's also consider another use for them. It's easy to imagine a targeted trojan running on a payroll manager's computer inside a Fortune 500 company, logging keystrokes, taking screenshots, and responding to commands from someone on the other side of the world – or someone just next door. Add me to your payroll, please. A bit far-fetched? Hopefully your organization has the proper policies and procedures in place to prevent this.

When the early reports of hackers teaming up with organized crime first surfaced, I'll admit I was skeptical. I found it hard to imagine a geek, albeit a criminal one, meeting up with the mob in a dark alley somewhere and plotting their next attack. But we're talking big money now, millions and tens of millions of dollars in some of the trojan-phishing-botnet-spam scams. Maybe much more. The link to organized crime and traditional low-tech criminals for cyber criminals is more likely one of pure necessity – converting "virtual money" stolen from individuals and companies still has to be converted to real money, and that's where traditional crime rings and money laundering come into play.

Law enforcement is pretty good at investigating the low-tech end result of high-tech crime, and that's where they should continue to focus. Rather than turn police officers into hackers, they should continue to work with (and pay) security people to unravel the technical capabilities. Let me put some emphasis on paying security folks for their hard work.

The lighter side of profit making

One cannot deny the allure of big profit, low risk cyber crime. It's a shame that hackers aren't paid more heartily for legitimate work like developing new applications, securing networks, building new web businesses, and so on. I want to believe that few people go out intending to be criminals, but the disparity between legitimate pay for legitimate work and the criminal profit is sometimes too great. It's scary, in fact, how much cyber crime has grown in recent years – even if the hard numbers and the Gartner polls are lagging behind the reality, I am not going out on a limb here. The FBI estimates cyber crime at somewhere around $8 Billion in the past two years against U.S. businesses. The world number is surely larger.

Would there be less crime if developers and hackers were paid more? If the Internet bubble hadn't burst? I'm not sure. But it's worth some thought.

On the complete opposite end of the spectrum are the people with great ideas who build something new and get paid outrageously well for their work. The folks at YouTube may have made off like bandits (accompanying video), but they are an inspiration for everyone in the Internet age. A small company of 65 people, which never turned a profit, was purchased for $1.65 Billion dollars in Google stock. That's the equivalent of 50 modest half-million dollar homes for *every single employee*. That's about about 1,159 Mini Cooper S-Type cars stacked end-to-end, for every single one of those hard working 65 employees. That's about... well, you get the idea.

Of course, I don't imagine the secretary of YouTube made off with $25.4 million dollars, because not everyone is equal... and not everyone's brain can be purchased for the same price. At $1.65 billion dollars for a 65 employee company, do you think Google really liked YouTube's ideas?

We can't all hope to win the Internet lottery like the folks at YouTube did, but I hope it's a sign of things to come: new investment in Internet technologies by big companies. Maybe if there's a little more incentive for a developer to be creative and create something new, instead of working on that new trojan-virus-spam-phishing scam in his spare time, some of the misguided virus folk might be inspired by some legitimate grandeur and cash, and not be headed to the dark side after all. Maybe? Maybe not? Well, one can only hope.