



Criminal Team Ups: Virus Writers for Hire?

infectionvectors.com

August 2004

Much like many kids, one of my favorite TV heroes was Batman. I loved the live action show, cartoons, comics, and the movies. Some of my favorite episodes of Batman, in any form, are the ones where multiple villains team-up against the Dark Knight. Although I always knew that Batman couldn't lose one of these fights, the combined evil brilliance of the Joker and the Riddler at least made me a little nervous. It's the same hollow twinge I feel for the virus writer "team-ups" warnings in the security media. Viruses are incorporating new and varied technologies, however, they aren't threatening any secret doomsday weapons that can't be stopped by the vigilant security administrator. What is scary about this cooperation is not the immediate threats, but the change to the entire security environment.

In a recent article on spam, an IT manager is quoted as saying, "If the spam people and the virus people got together, we could have a big problem." [1] That certainly sounds threatening, but we've managed to get through it so far. Since SoBig, a number of viruses have installed mail (spam) relays onto victim machines. [2] So viruses have installed spam engines, and we're waiting for spam to drop Trojans on our machines (although, that would probably cinch up my disinterest in whatever product was being advertised) [3].

Spammers generate revenue by spamming, that's the simple nature of their business. I'm no economics professor, but I am willing to bet that if there was no money in it, there would be much less interest in spamming. It was a natural fit to take the successful mass mailer worm (and its efficient SMTP engine) and combine it with a need to send out millions of anonymous messages. Using mass mailers with emailed notifications of infection success back to the authors makes sense, the best way to verify that a host machine is not prevented from sending email directly to the Internet is to use email as the alert mechanism [4]. The spammers are still at it, now incorporating the rapid-propagation techniques of Internet worms in such incarnations as Bobax. [5] The collusion between the spamming industry and the underground virus factories is significant because it makes virus writing a profession. The important team up is not between the spammer and the virus coder, but rather between money and the virus coder. Now breaking into boxes, any boxes, represents real money.

All Aboard

The team-ups of the future will probably mirror those of the past: a virus writer with a particular interest for mischief or a prankster with an interest in virus writing (virus "tweaking" is more likely). If there is a financial interest in the crime, however, that

analysis goes out the window. Money has an amazing power to drive criminal acts, as long as there is a means to carry it out (guns, cars, skill evading detection devices, insert your favorite crime film's plot here). The virus can become the vehicle that propels the crime. A means and a motive are the two ingredients for a crime most of us recognize from courtroom TV shows. A criminal needs a mechanism and a propensity to commit the crime. The propensity could be purely personal, an evil nature. Or, it could be coaxed out by financial gain. The mechanism is presenting itself in new forms everyday by way of published worm source code and the new samples that can be disassembled, modified, and rebuilt without expensive tools or a lengthy formal education.

Whether the crime is vandalism, robbery, or anything else, the addition of a financial motive will propel the "industry" to new heights. There is little money in DoS'ing Microsoft.com or SCO (at least right now). However, including such things in the MyDoom variants go to show that the addition of talented virus writers and the desire to knock out a particular domain can be a powerful combination. If someone was willing to pay a good deal to knock over a domain, I suspect the task would not take too long to complete.

We've already seen the combination of virus writers and vandalism; web defacement has been the goal of worms released this year such as the most recent variants of Welchia. [6] When it comes to making money from infecting machines with a virus/backdoor combination, the money exists as well. Selling compromised boxes for whatever purpose has gone on for years [7].

Powerful Team Ups?

What team-ups are coming? The most intriguing is probably the merging of virus writers and skilled cryptographers. As has been seen with encrypted worms like variants of Beagle, virus scanners are little use against unreadable files. The polymorphic crypto-virus is likely to scare a number of security administrators.

As a whole, the collusion possibilities are unlikely to generate a lot of actual products. It seems reasonable to think that virus coders will simply learn new skills as necessary, with the abundance of reusable code and technical manuals available.

Legalize Spam?

Most of the arguments for legalizing drugs eventually point out how much money we spend as a nation prosecuting and locking up drug offenders. Furthermore, there has been a great deal of consideration given to the financial incentives of selling drugs and its correlation to the amount of organized crime built up around drugs. The impact of this crime extends far beyond just selling more drugs; the violence surrounding the drug trade is well known. If it becomes equally well accepted that the blocking and criminalization of spam has created an anonymous empire of viruses, will the same arguments surface? Maybe we'll start wishing for the good old days when spam was just annoying. I doubt it. The cost of spam, not to mention the security threats presented by Trojans and viruses

will never low enough to justify forgetting about them. Besides, no matter the team up against him, Batman would never give up on spam.

References

1 The quote is from “Information Security Magazine” May 2004. The article is available at http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss386_art765_00.html.

2 The SoBig mass mailer details are available at any antivirus vendor site. A great report on the different variants is available at Lurhq: <http://www.lurhq.com/sobig-e.html>.

3 This has most likely already happened, and certainly has if your definition of Trojan includes spyware, adware, etc.

4 That way, a host that reports back to the author has already proven that it can be used as a relay. Using IRC to notify the author does not positively indicate that the host is allowed to send email (TCP 25) to the Internet directly.

5 I again point to a very good report at Lurhq: <http://www.lurhq.com/bobax.html>.

6 Maybe a political message in the form of the rewriting of web pages on Japanese servers: <http://www.sophos.com/virusinfo/analyses/w32nachib.html>.

7 A couple of news items that mention the sale of compromised machines:

http://www.wired.com/news/infrastructure/0,1377,62324-2,00.html?tw=wn_story_page_next1

http://www.theregister.co.uk/2004/02/22/trojans_as_spam_robots/

http://www.theregister.co.uk/2004/04/30/spam_biz/

Batman is a registered trademark of DC Comics.

For reprint rights contact@infectionvectors.com