available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The metamorphosis of malware writers

Danny Bradbury

ARTICLE INFO

Article history:
Received 20 January 2006
Revised 23 January 2006
Accepted 23 January 2006

ABSTRACT

The reasons for writing malware are changing – and so is the malware itself. Danny Bradbury reports on the development of a seedy commercial market.

Bill Gates' time is up. At the end of January 2004, at the Davos forum, he said that within two years, spam would be a thing of the past. In reality, the problem is as rampant as ever. On its own, that would be merely irritating, but for the past three years or so, developments in the relationships between spammers and malware writers have followed a worrying trend. Security experts agree that the two are colluding for profit, meaning that the motives and modus operandi of malware writers have been changing.

"When I started in 1988, people were writing viruses and malware mostly to become famous," recalls Righard J. Zwienenberg, Chief Research Officer at security software vendor Norman Data Systems. "Nowadays it's moved from that field into the more organised crime field."

Botnets are largely responsible for bringing spammers and malware authors together. Known to most people working in security today, botnets are networks of compromised 'zombie' PCs which can be exploited by hackers for nefarious purposes. Networks of compromised servers were used from 2000 onwards for distributed denial of service attacks, but in the early days the motives were either just for the thrill of it, or to attack a political target such as an SCO, which was hit by a DDoS attack after taking a contentious legal position against Linux users.

Security experts such as Miko Hypponnen, head of anti-virus research at security firm F-Secure have said that 2003 was the year when things changed in a big way. The use of botnets became more organised as spammers realised that instead of relaying email through unprotected corporate SMTP servers which would soon be blacklisted, they could use thousands of PCs to send unsolicited commercial email. The malware writers who compromised the computers with Internet worms realised that they could be rented out to spammers for a fee. As botnets created from compromised desktop PCs grew, they created a black market in zombie machines manipulated via IRC to send spam. "We're seeing more evidence than ever before of that organized element coming into virus writing," says Graham Cluley, senior technology consultant at Sophos.

If sending spam from an unwitting users' PC was not bad enough, other for-profit uses of botnets are even more sinister. "The Russian mafia is pretty well known nowadays, operating botnets to get details from credit cards," says Zwienenberg. A compromised desktop PC can be programmed to log keystrokes and look for credit card numbers, for example, or monitor access to banking websites to harvest passwords. The Bancos Trojan, released early last year, is a good example of such an attack.

For this reason, the nature of malware is changing. Internet worms designed to spread quickly were commonplace a couple of years ago, but 2005 saw fewer of these, says David Emm, senior technology consultant at anti-virus vendor Kaspersky Labs. "What we saw instead is where people want to send out malicious code, they're spamming it deliberately," he says. "They do an initial spam distribution and that's it. So the thing doesn't has legs of its own, it relies on the first blast."

The reason is twofold, explains Sophos' Cluley. Firstly, sending out a rapidly proliferating worm to create a huge botnet is too obvious and raises too many alarms, prompting users to take security measures. Yesterday's hobbyist malware writer was generally an adolescent male wanting to be noticed by his peers. Today's for-profit malware writers want to stay under the radar, because if their product is noticed it prompts victims to take action and reduces

E-mail address: danny@itjournalist.com

0167-4048/$ – see front matter © 2006 Published by Elsevier Ltd.
doi:10.1016/j.cose.2006.01.003

the number of compromised machines. This is why modern malware is less likely to deliver a payload obvious to the victim, such as deleting files from the hard drive. Organized commercial malware authors want to enslave, not destroy, their targets.

Secondly, while it may be advantageous to co-opt as many PCs as possible to a botnet used for a DDoS attack, large numbers of zombie machines can be counterintuitive when using them for other purposes.

"If the botnet does steal credit card information, [a very large botnet would provide] too much data for the criminals to handle," points out Cluley. "They don't want a million credit card numbers because that is too many to process." Better to steal credit card numbers from 100 zombie machines, process them, and then create another 100 zombie PCs at your leisure.

No wonder, then, that Sophos has seen a surge in the number of non-replicating Trojan horse programs being spammed out by email. Sixty-two percent of all malware programs that the company saw in 2005 were Trojan horses.

This does not mean that DDoS attacks are a thing of the past, however. They have also evolved into a commercial venture for criminals. Companies such as online gambling sites and banks are receiving blackmail threats from criminal groups who threaten to bring down their websites for periods of time using botnet-originated DDoS techniques. Apart from the loss of face and customer confidence, this can also have a serious impact on revenue if, for example, an online betting site is taken down just before a high-profile sporting event.

Another trick that F-Secure's Hypponnen identified over a year ago was the use of botnet machines to host files. In one case, he found that crooks using some of the rarer top-level identifiers such as .biz and .info were able to reduce DNS caching times to minutes, meaning that the destination machine behind an URL could be changed very quickly. Several machines on a botnet could then be loaded with content and used as temporary servers, making it difficult to shut down an illicit website.

Such illegal websites can be used for activities such as selling counterfeit software. Peter Anaman, a senior Internet investigations manager who traces counterfeit software vendors for the Business Software Association began noticing botnets being used to host illicit websites last July. However, in the version he saw, the content did not reside on the compromised desktop PC. Instead, it resided on a server, which could be replicated in different regions to throw investigators off the trail.

"Virus writers would offer infected computers on these botnets, and once they were infected they acted as web proxies," he says. "Every time you did a reverse lookup to find out where something was hosted, you'd find a DSL account."

The people behind such cybercrimes come from multiple countries. In some cases, Anaman is convinced that organized crime groups associated with other physical crimes are also engaging in online crime.

"Brazil is particularly the staging post for some of this stuff," says Kaspersky's Emm. "We have also seen activity coming out of the far east and Russia." Some of the Russian malware encrypts data on the target machine and then asks the user for money in return for a decryption tool to return the user's data.

While such malware hides files and holds them to ransom, another kind does exactly the opposite, recovering sensitive files from PCs and delivering them to the attacker. The National High-Tech Crime Unit in the UK arrested London-based Michael Haephrati in 2005 as part of a law-enforcement exercise called Operation Racehorse. Haephrati was accused of supplying a Trojan horse program to hackers which would harvest confidential documents from a PC. Executives in several Israeli companies were placed under investigation for corporate espionage.

Wherever they are from, it is likely that cybercriminals are using a different generation of malware writer to the typical maladjusted teen who has traditionally been the author of viruses in the past. Sophos has not seen any evidence of known virus writing groups such as 29A working with criminals – indeed, 29A is now largely dormant. Young people with computer skills who are not ethically mature may realise that they can make money from their activities, says Cluley. "Whether the serious organized criminals would want a teenager on their books or not is another question. They might make mistakes or brag about it. So I think the demographic is getting older."

Detecting and catching cybercrooks can be difficult. "They use thousands of domain names registered worldwide through different registrars," says Anaman of the criminals using botnets as proxies to illegal websites. "These are kept in hibernation until used. Those in hibernation, which is a good 75% of them, are harder to find."

Anaman will adapt standard network tools in innovative ways to help gather evidence. For example, he may conduct a batch WHOIS lookup to find all of the domain names registered by the same person and try to cluster registration information and identify trends.

But even after these efforts it can be difficult to pin down the perpetrators. "We have had a lot of problems because once you have crimes committed across borders, although there is great co-operation between countries it isn't as refined as it should be," Anaman says. "So a lot of cases have to be dropped because there isn't enough evidence in a particular country to support it."

In England, the National High-Tech Crime Unit worked extensively with authorities in other countries to try and tackle the problem, but it is an uphill battle. The Internet's strength is a weakness for law-enforcement agencies. Electronic Frontier Foundation co-founder John Gilmore said in 1993 that the Internet treats censorship as damage and routes around it. That may be true, but what applies to censorship may also apply to law enforcement. And as malware writers become more commercially minded, that could make the Internet the battleground of the 21st century.