Report on Computer Worms and Viruses in 2004

by Christopher J. Hazard

In terms of computer worms and viruses, 2004 was the advent of the computer worm business model. Worms are generally defined as a program which replicates across a network on its own, whereas viruses are usually defined as code which attaches itself to executables and requires them to be actively run in order to replicate. The difference between worm and virus is not always clear, and the two terms are often used interchangeably. Trojans are defined as programs which somehow trick the user into running them, and in doing so perform unwanted behavior. Mobile phone worms made their first appearance. Worms had new behaviors such as removing other worms and making worm analysis more difficult. And, several worms were released very quickly after exploits had been discovered. In this paper, I will present a summary of the behavior of worms and viruses in 2004.

The number of viruses has been constantly growing since they were first invented, and 2004 was no exception. It was widely recognized that over 100,000 viruses were known in 2004, an increase of 20-50% which varied by news source [1,2]. This number is meaningful in terms of representing the large number of viruses found in the wild, but is possibly exaggerated slightly. One exaggeration is that variants of the same virus family are counted separately. This counting method is useful in many cases, as the two viruses may be different. However, if a minor bug is fixed in a virus which only makes it spread slightly faster, it is more difficult to argue that they are different apart from their signatures. Another potential exaggeration is virus naming conventions. Though virus family names are generally agreed upon, co-discoveries of virus variants can sometimes lead to name overlaps, as well as general confusion [3].

2004 also marked the expansion of a new motivation for virus creation: profit. Previously, viruses were usually created out of malice, curiosity, extortion, lust for power, or harming competitors in a commercial setting [4]. This new motivation comes as a market solution for problems faced by spammers. Historically, spammers have had to maintain their own internet connections from which to send spam. Ostracizing by internet service providers, coupled with new anti-spam laws, has made obtaining and maintaining these centralized spam outlets difficult and costly. The power of free markets found a solution to this problem. By hiring virus writers to create viruses that infect and control large numbers of PC's, spammers can have easy access to an ultra-high bandwidth, decentralized, spam-sending machine. 2004 was not the first year that these worms were released. In 2003, Sobig, Slanper, and Trojanproxy exhibited this behavior, and Fizzer would turn an unsuspecting computer into a for-profit webserver [5].

The two main SPAM viruses of 2004, Bagel and MyDoom, were also two of the most prevalent viruses. Both turned infected PC's into SPAM proxies, and both viruses had many variants [1]. In addition, these viruses utilized the same Mitglieder trojan, leading anti-virus firms to suspect that they were created by the same group. MyDoom had additional malice, with variants performing distributed denial of service (DDoS) attacks against various websites including www.microsoft.com, www.sco.com, and www.riaa.com. In light of events around the SCO Unix ownership lawsuit and Microsoft and RIAA practices, the BBC published an article suggesting that Linux zealots created this virus [6]. This lead to outrage on the major online technology oriented discussion community Slashdot [7]. A later variation of MyDoom used Google to scan for e-mail addresses. Both Bagel and MyDoom shared many malicious tricks to fool the user into opening their malicious e-mail attachments. Though they were executables, they used icons that represent less harmful file-types such as folders and word documents. Bagel used zip files to prevent antivirus programs from detecting it. Once antivirus vendors caught on, it started encrypting the zip files with a password sent in the e-mail, and finally e-mailed a rendered image of the password [1]. Other viruses began to exploit MyDoom's backdoor, notably Doomjuice and Deadhat [8].

The idea of an antivirus virus is not new, and the notion of competing processes has been around since CoreWars. In 2003, the Welchina worm actually cleaned out the Blaster virus, downloaded legitimate security patches that protect against Blaster, and installed them [9]. Though this spawned debate of the legitimacy of "friendly" worms, it was still very problematic for infrastructure. In 2004, the Netsky worm took worm warfare to a higher scale. Netksy spread in a similar way to Bagel and MyDoom, but attempted to remove both Bagel and MyDoom from the system. This turned into a war between the writers of Bagel and MyDoom, and Netsky. Each group released many variants, containing flamewar messages against each other in the virus code [10]. The Netsky group thought they were doing everyone a favor by destroying worms that are used to send SPAM, that they respected antivirus companies, and also indicated the final variant of the virus. Following Netsky, the Sasser worm had similar behavior in that it attempted to remove Bagel and MyDoom, but was able to spread much faster. Sasser rebooted computers and caused enormous havoc, leading some security firms to label it as the most destructive worm yet. The Sasser author, an 18 year old named Sven Jaschan, was quickly arrested by German police. After his arrest, versions of MyDoom were released containing comments that mocked and taunted Jaschan [11]. Even after Jaschan's arrest, several more variants of Sasser were released [12], suggesting that there were more individuals behind this worm.

Jaschen was one of many virus writers arrested in 2004. 2004 had the largest number of virus writer arrests [1]. Virus writers were caught in a variety of countries including Russia, Germany, USA, and Canada. Organized crime increased of trafficking credit card and banking information. Though not directly related to worms, it is worthwhile to mention that a number of phishing scammers were also arrested, and two major credit card number trafficking sites were shut down by the US Secret Service [1]. Several worms were created with the intent of stealing such information. Although not widespread, the Korgo worm logged web-form information such as bank account numbers [13], and could be controlled to retrieve this information via commands sent over IRC servers [14]. Opener, another malware program that logged keystrokes, was notable for being the first real threat to Apple's OS X system. The Opener shell script downloaded software to aid in breaching security, disabling system accounting, and turns on file sharing, but needed to be initially deployed as root. The classification of this shell script was heavily debated because of its weak ability to replicate itself [15]. Apple Computer dismissed it as not threatening, but the firm Sophos Plc, a maker of software security systems, classified it as a worm.

Organization and competence of malware authors was also notable in 2004. The Bofra worm was released only a few days after a vulnerability was announced in Internet Explorer [16]. The worm coerced users to click on a web link back to the infected machine that sent the e-mail, and used the exploit in Internet Explorer to find e-mail addresses on the host machine, setup a server hosting the malicious webpage, and sent e-mails pointing back to it. Though the Bofra attack was quick and organized, the Witty worm was far more impressive. The Cooperative Association for Internet Data Analysis published a concerning analysis of the Witty worm [17]. Witty was released only one day after a vulnerability was publicized in ISS products. This vulnerability was in proactive security software, such as BlackICE, making Witty the first worm to ever target security measures. ISS software is only run on a relatively small population of the internet, which showed the viability of a worm impacting systems without monoculture. It also was the first widespread worm to actively cause destruction to information, done by randomly deleting sections of the hard drive. Witty also targeted a large number of vulnerable hosts right away, meaning that the worm deployers must have found these targets a priori.

The Atak worm, like Witty, had its own novelty. The Atak worm was not particularly dangerous. Nor did it generate much media attention. However, the Atak worm contained code that detected whether or not it was running in a sandbox. The supposed author was an Al-Qaeda sympathizer that had threatened to release an "uber-worm" if the US attacked Iraq [18]. Major security companies indicated that it was difficult to discern its behavior, and admitted to not knowing its precise behavior [19]. Panda Software scoffed at the attempt: "But any researcher worth his salt will blow right past that." [20]. Even if Atak's discovery prevention methods were not difficult, it does present the possibility of worms using clever tactics to add difficulty to the antivirus companies. If internal antivirus company technologies became known to worm writers, they could possibly lengthen the time antivirus companies take to deploy solutions. Also notable about this story is its discussion on the online community Slashdot [21]. Here was a large discussion involving the prospects of what previously unseen attributes would make a virus extremely harmful. One of the major conclusions was that worms that showed no noticeable behavior to the user, but slowly changed numbers and figures in excel spreadsheets and word documents could do the worst damage. If the data spreadsheets are slowly and unknowingly changed, it will continuously be backed up. Companies could base business decisions on corrupted data. When the data is found to be corrupted, it could be difficult to figure out when the data was initially corrupted, and what data was changed by the malware, and what was intended to be changed.

The notion of getting a worm or virus simply by opening a picture was laughably ridiculous up until recently. However, in September 2004, Microsoft revealed a vulnerability in their JPEG libraries. There was a bit of media buzz about this prospect, discussing various ways this exploit could be easily utilized [22]. Luckily, the worst thing that happened was a failed attempt at an AOL Instant Messaging worm that attempted to use this vulnerability [23]. The worm was not widespread. This type of non-executable data exploit is concerning, and future attacks could potentially exploit bugs in libraries that load data files of music, images, and documents.

Another type of new virus medium in 2004 was mobile devices. The first one found in the wild was Cabir [24], which propagated over Bluetooth communication. This is particularly notable because it can only spread between devices that are in close proximity of each other, akin to the way human airborne viruses spread. Though its current actions are benign, a wide variety of variants have shown up, making some worry that its source code is being shared. Mosquito was a more malicious Trojan which sent SMS messages to premium priced numbers, incurring cost on those infected [25]. Skulls is another Trojan that renders mobile phones unusable [26]. Duts was another proof of concept virus that targeted Pocket PC's which prompted the user to allow it to spread [27]. Though all of these mobile malware programs posed little real threat, they may be an indication of the future malware.

The last major worm of 2004 was Sober.I [28], which began in 2003 and has had many variants. Sober's e-mail messages vary in content between the German and English versions. The English version is rather tame, but the German message claims to be from a model looking for work, with pictures attached.

Traditional computer viruses, which infect executables and propagate as they are run, have become almost non-existent. Only ten are known to remain in the wild, and are, amusingly, propagated by riding on the back of worms [29]. If a user has a traditional virus and also gets infected with a worm, the worm's code in turn may become infected with the virus. When the worm propagates, the virus comes along, and is executed on the newly worm-infected computers. Most antivirus software packages were designed to combat these traditional types of viruses. Worm infections have been exploding over the course of hours, and antivirus companies do not have time to act. Some, including Kaspersky Labs, think that it could be time to re-think worm detection strategies and use more general intrusion detection heuristics [30].

References

1. *F-Secure Corporation's Data Security Summary for 2004*. (2004) [online] F-Secure Corporation. Available from: http://www.f-secure.com/2004/

2. Ward, M. (2004) *Cyber crime booms in 2004*. [online] BBC News UK Edition. Available from: http://news.bbc.co.uk/1/hi/technology/4105007.stm

3. Brenner, B. (2004) *Caught in the virus name game*. [online] SearchSecurity.com. Available from: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1024919,00.html

4. Nicholas Weaver, Vern Paxson, Stuart Staniford, and Robert Cunningham. *A Taxonomy of Computer Worms*. In First Workshop on Rapid Malcode (WORM), 2003.

5. *F-Secure Corporation's Data Security Summary for 2003*. (2003) [online] F-Secure Corporation. Available from: http://www.f-secure.com/2003/

6. Evans, S. (2004) *Linux cyber-battle turns nasty*. [online] BBC News World Edition. Available from: http://news.bbc.co.uk/2/hi/business/3457823.stm

7. Carless, S. "simoniker". (2004) *BBC Links Linux To MyDoom*. [online] Slashdot. Available from: http://linux.slashdot.org/article.pl?sid=04/02/05/0818229&tid=88&tid=106

8. Lemos, R. (2004) *Doomjuice, Deadhat feed on MyDoom infections*. [online] ZDNet Australia. Available from: http://www.zdnet.com.au/news/security/0,2000061744,39116051,00.htm

9. Naraine, R. (2003) *'Friendly' Welchia Worm Wreaking Havoc*. [online] internetnews.com. Available from: http://www.internetnews.com/ent-news/article.php/3065761

10. Kotadia, M. (2004) *Netsky author signs out with final variant*. [online] ZDNet UK. Available from: http://news.zdnet.co.uk/internet/security/0,39020375,39148153,00.htm

11. Warner, B. (2004) *Net Virus Turf War Resumes*. [online] From Reuters hosted by NetSecure, Ltd. Available from: http://www.netsecureglobal.com/SITE_Default/Case_Studies/040917_Virus_Turf_War.asp

12. Jaques, R. (2004) *Sasser strikes back despite arrest*. [online] WhatPC? Available from: http://www.whatpc.co.uk/news/1155010

13. Farrell, N. (2004) *Korgo worm targets bank accounts*. [online] The Inquirer. Available from: http://www.theinquirer.net/?article=16341

14. Naraine, R. (2004) *Korgo Worm Targets LSASS Flaw*. [online] internetnews.com. Available from: http://www.internetnews.com/dev-news/article.php/3359681

15. Gibson, B. (2004) *TMO Reports - Apple: 'Opener' Worm Not a Virus*. [online] The Mac Observer. Available from: http://www.macobserver.com/article/2004/11/02.2.shtml

16. *Warning issued over Bofra virus*. (2004) [online] weboptimiser. Available from: http://www.weboptimiser.com/search_engine_marketing_news/6094910.html

17. Shannon, C., Moore, D. (2004) *The Spread of the Witty Worm*. [online] Cooperative Association for Internet Data Analysis. Available from: http://www.caida.org/analysis/security/witty/

18. Kotadia, M. (2004) *BitDefender sees Al-Qaeda link in new Atak worm*. [online] ZDNet UK. Available from: http://news.zdnet.co.uk/internet/0,39020369,39160707,00.htm

19. Kotadia, M. (2004) *'Smart' worm lies low to evade detection*. [online] ZDNet Australia. Available from: http://news.zdnet.co.uk/internet/security/0,39020375,39160285,00.htm

20. Keizer, G. (2004) *Worm Tries To Foil Anti-Virus Researchers*. [online] InformationWeek. Available from: http://www.informationweek.com/story/showArticle.jhtml?articleID=23900539&tid=13692

21. Lord, T. “timothy” (2004) *'Stealth' Worm Hinders Sandbox Analysis*. [online] Slashdot. Available from: http://it.slashdot.org/article.pl?sid=04/07/14/1419250&tid=172&tid=128&tid=201

22. *JPEG Exploit Hits Usenet, Worm Close Behind*. (2004) [online] TechWeb. Available from: http://www.techweb.com/wire/security/47903375

23. Evers, J. (2004) *Instant messaging worm exploits JPEG vulnerability*. [online] Computerworld. Available from: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,96268,00.html

24. Festa, P. (2004) *Cabir cell phone threat worsens*. [online] CNET News.com. Available from: http://news.com.com/Cabir+cell+phone+threat+worsens/2100-7349_3-5505854.html

25. Thompson, I. (2004) *Mosquito Trojan set to infect mobiles*. [online] vnunet.com. Available from: http://www.vnunet.com/news/1157233

26. Lemos, R. (2004) *Skulls program kills cell phone apps*. [online] CNET News.com. Available from: http://news.com.com/Skulls+program+kills+cell+phone+apps/2100-7349_3-5460194.html

27. *First Pocket PC Virus 'Poses No Threat'*. (2004) [online] TechNewsWorld. Available from: http://www.technewsworld.com/story/35220.html

28. Kawamoto, D., Ilett, D. (2004) *Sober worm variant shimmies*. [online] CNET News.com. Available from: http://news.com.com/Sober+worm+variant+shimmies/2100-7349_3-5459834.html

29. *Where We've Been and Where We're Going*. (2005) [online] Kaspersky Lab. Available from: http://www.viruslist.com/en/trends

30. Emm, D. (2004) *Traditional antivirus solutions - are they effective against today's threats?* [online] Kaspersky Lab. Available from: http://www.viruslist.com/en/viruses/analysis?pubid=153595662