CLEARSWIFT™
Managing and securing
electronic communications

ThreatLab 2003 Retrospective

The Year the Mafia Moved In

Table of Contents

Introduction

2003 was a quite extraordinary year in the malware world. Three major developments went largely unrecognised:

- the emergence of long-term malware projects, involving multi-stage attacks using spam, worms, trojans, spyware and proxies
- a clear switch in motivation - no longer intellectual challenge or simple-minded cyber-vandalism, but financial gain became the primary motive
- the emergence of a covert peer-to-peer malware network.

As traditional virus-writing groups went deeper underground or disbanded, organised crime, by stealth, undertook a radical redrawing of the malware landscape.

Historically, hackers (of the 'Black Hat' persuasion), virus writers and spammers formed discrete communities. In a hierarchy, based on technical ability, the hackers looked down on the majority of virus writers, as 'script kiddies' and everyone looked down on the pond life called spammers. In 2003 we witnessed a convergence of the three skill sets, not because these three communities suddenly decided to cooperate, but because organised crime groups deployed the tools of spammer, virus writer and hacker in a co-ordinated manner to expand their operations into cyberspace and to explore new opportunities for criminal activity.

Any retrospective commentary for 2003 would be incomplete without an obligatory nod to Slammer and Blaster (Welchi etc.). These high profile events, however, made their impact by virtue of the novel infection vectors: SQL and DCOM RPC. They caught the antivirus companies unawares, broke existing records, hit the headlines, but were isolated incidents of little real, long-term consequence. In the main their impact was the side-effects of network congestion. We shall return to them later in a broader context. Sobig.F attracted media attention, but in contrast, was part of a longer-term project - one of several.

The Sobig Project

In August, the mass-mailing worm Sobig.F attracted widespread media attention by virtue of the truly massive amounts of mail it generated. However, it's real significance was not widely appreciated. Between January and August six versions of Sobig were released as controlled experiments, each with the exception of the first (Sobig.A) having a self-imposed termination date and each designed as the first step in multi-stage effort to subvert tens of thousands of insecure PCs for nefarious purposes.

The end game was the creation of an army of hidden proxies from which to relay spam, but the details of the steps leading to that end are interesting. Sobig worms were classic mass-mailers, spammed out at the seeding stage. The worm used simple but effective social engineering to entice unwary recipients to execute the code by clicking on the attachment. Once installed on the PC, Sobig would monitor the contents of a file on a remote web page at Geocities or in later versions, on hacked cable modems. For brief periods, it would contain the address of another remote file - the Lala trojan, which Sobig would download and run as the second stage of the operation. The Lala trojan would then notify its location to another remote site and download a keylogger, a remote access trojan and a custom installer for the Wingate proxy server (a legitimate product used without licence). With the third stage - installation and configuration of the Wingate proxy - the process was complete and the PC ready to perform the wishes of its new (remote) owner. No trace remained of the initial Sobig worm and, because of extreme stealth, users would almost certainly be oblivious to the hijack.

One of the several functions of the Lala trojan is to monitor Internet Explorer pages containing the text "e-gold Account Access", "Account Access", "Bank", "My eBay", "Online Service", "bank", "E*TRADE Financial" or "PayPal - Log In". If found, it activates the keystroke logger to steal usernames and passwords. Clearly, identity theft, credit card fraud and ebank robbery are all on the agenda.

The large increase in spam volumes in 2003 is, in no small part, due to the installation of proxies by Sobig. Currently, about two thirds of spam is spawned from compromised broadband PCs. At each successive release of Sobig, the weakest link in the process has been the vulnerability to rapid closure of the second stage web location of the Lala trojan. Indeed intercession by law enforcement to take down the twenty sites hosting stage two instructions resulted in the complete failure of Sobig.F. Despite, the vastly increased spreading rate of the F version, a week's delay before the onset of stage two proved its undoing.

Sobig, as a sideline, targeted online banking customers, but Bugbear.B targeted employees inside the networks of about 1300 banking and financial institutions.

Phishing Expeditions

Phishing spam increased enormously in the last quarter of 2003 and most major banks in the US, UK and Australia have been targeted.

'Phish' is an old term for accounts that have been hacked. More recently 'phishing' has come to be used to refer to attempts to steal financial credentials by fooling a user into believing that the have received a bona fide email from an ebank or payment system such as PayPal.

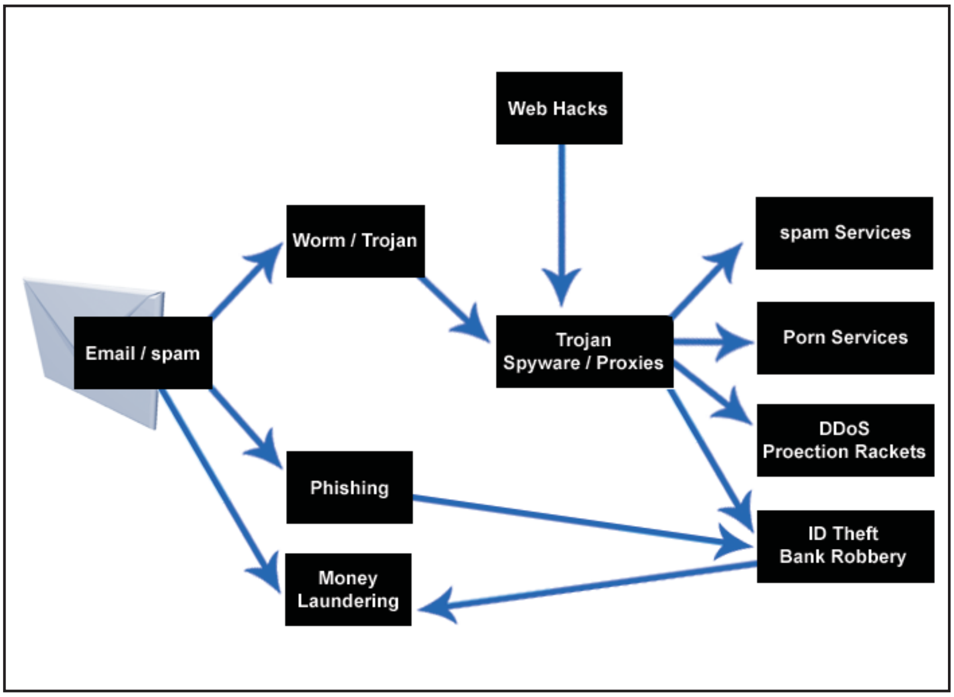
In the simplest case the email itself may have an HTML form that requests verification of banking credentials. More sophisticated attacks may contain a URL link to a web page closely mimicing that of the real ebank, most recently exploiting a flaw that displays the real site's URL in the address bar of Internet Explorer. Alternatively, some display a pop-up requesting credentials, whilst redirecting to the real ebank page. Yet a fourth ploy included a trojan keylogger as an attachment to the spam, which opened a link to the real bank login page, captured credentials as they were typed in and emailed these to a dead drop account, if the user actually logged in.

By far the most prolific assaults on online banking were mounted by a group of unknown individuals, recognizable as a unit due to the unique format of mail headers generated by their spamming tool. These have targeted customers of Citibank and Ebay repeatedly since September and in late October targeted customers of the UK high street banks - Barclays, Nationwide, Halifax and NatWest.

The Mimail Project started in August with a harmless but fast spreading worm. This developed into versions attempting denial-of-service attacks on anti-spam blacklist sites such as Spamhaus.org. Then in November, Mimail.I targeted PayPal customers with a notification that their accounts would expire within five days unless credentials were confirmed.

Phishing activity escalated dramatically over the last two months of 2003 to a peak of five new unique, fraudulent email reports per day over the Christmas period. At the same time they have increased in sophistication and many trace back to Russia and Eastern Europe.

The Bigger Picture



The vast and growing pool of unprotected, broadband-connected home PCs represents the soft underbelly of the Internet. However, given the shotgun approach to spamming malware, many small-medium (and a few large) businesses are equally vulnerable. Organised criminal groups have come to value these resources as a base for diverse money-making operations. Control of tens, if not hundreds, of thousands of these PCs has fallen into the hands of criminals.

Infiltration has been achieved in a number of ways. As neophytes connect their new PCs to the Internet, the chances are very high that these will be identified as easily hackable, by automated scanning tools within the first day. Some may have personal firewalls, but these offer little protection against spammed email containing worms and trojans. Many systems were left wide open to remote attack by the Blaster worm, which opens a remote shell on port 4444. Numerous unpatched vulnerabilities in Internet Explorer, expose surfers to drive-by attacks as they view malicious web pages, leading to the silent installation of trojans and spyware.

Infiltration has been followed by the capture of banking and credit card information, leading to ebank robbery and identity theft. Installation of proxy servers has opened up several opportunities for financial gain, the first of which to be exploited was the ability to mount anonymous spamming operations. Not only does this take the game full circle, facilitating the further spamming of worms and trojans, but services have also been offered to traditional spammers, at a price.

Proxies on these 'owned' PCs have also been used to front untraceable pornography sites, soliciting subscriptions, potentially leading to further theft of credit card credentials. The most audacious abuse so far has involved protection rackets, marshalling these resources to act as 'zombies' in distributed denial-of-service attacks on online betting shops, offshore casinos in the Caribbean and electronic payment systems such as WorldPay. Scores of small-to-medium sized companies have been threatened with attacks unless they pay relatively small protection fees.

The success of these criminal enterprises raises the challenge of laundering the proceeds and this provides clues to the origins and identities of the perpetrators. Spammed email offers have been targeted at customers of the Australian banks ANZ, National and WestPac. Posing as a legitimate Russian company, they offered customers a commission for allowing deposits to be made to their accounts, retaining 10% and transferring the remainder by Western Union. Those who took up the offer found that large sums were indeed deposited in their accounts, originating from other accounts in the same bank - a highly-effective (but difficult to monitor) means of money laundering.

Serotonin - "Its life, Jim, but not as we know it"

Whilst organised crime has come to dominate the malware scene, in 2003, the traditional virus-writing groups have not been entirely moribund. In Jan 2003, Serotonin, probably the most advanced worm ever written so far, was announced on the Underground. According to the author, a prolific virus coder, the worm took almost a year to write.

Why is it worthy of inclusion in a review of the year 2003, when it received no publicity and caused no direct damage whatsoever? Serotonin represents an entirely new generation of worm, using 'Genetic Programming' techniques, based on processes analogous to those operating in biological evolution.

Genetic Programming concepts are not new. The idea is to mimic natural selection processes, allowing small, random mutations (in the main debilitating or self-destructive) and novel combinations of pairs of genotypic material (as in sexual reproduction). It is not inaccurate to describe this a 'breeding'. The principle of survival-of-the-fittest then applies to the offspring. This allows for a degree of morphological change, quite different in character from the established computer virus techniques of polymorphism and metamorphism. It also introduces an element of functional creativity, whereby a one in a million event can result in some new characteristic that fortuitously enhances survival prospects.

The success or otherwise of these techniques, in-the-wild, may be of more than passing interest to evolutionary biologists. Nonetheless the cat is out of the bag - the code has been available on the Internet for some time. It would, perhaps, be a prudent move on the part of the antivirus research community to obtain the code and study its evolution closely in the controlled environment of the laboratory, rather than wait and see what eventually emerges outside.

But hold – this raises first order ethical issues. Most of the antivirus community are implacably opposed to creating viruses in an academic environment, in order to better understand them. Furthermore, the code for Serotonin is an unfinished proof-of-concept, so any serious academic study would necessitate writing additional code to make it optimally viable. Without wishing to reopen the University of Calgary debacle of 2003, it is worth pondering the ethical implications of research into genetic worms. Analogies with biowarfare research spring to mind.

Sinit - a Private P2P Malware Network

Early in 2001, the infamous virus-writing group - 29A - published proposals for a private, peer-to-peer, malware network (akin to the Kazaa and Grokster P2P networks). The proposed networked malware would use a simple communications protocol to exchange new versions of modules. To pre-empt the interventions of antivirus forces, communications were to be encrypted. The plan offered the virus-writer two main advantages: rapid dispersal of new code and removal of the single-point-of-failure, inherent in posting new code to one or more web sites, which could be closed down rapidly - the main flaw in the Sobig Project.

Someone put the plan into action, in late 2003. A covert P2P malware network has been ushered in quietly by the trojan known as Sinit, Fakesvc or BAM. A noticeable increase in malformed DNS traffic was first thought to represent a DNS-fingerprinting exercise, but was eventually identified as communications between the Sinit P2P trojan. Sinit exploits a known vulnerability in the Java VM, to download itself from malicious web pages.

Discovery of infected hosts is a simple matter, as they will respond readily to connection attempts on port 53. No single point of failure exists as new code can be introduced into the network at any point and reach all hosts. New code, however, is (ironically) digitally-signed by the developers of the network, preventing injection of neutralising or self-destructive code. Eradication may be no trivial matter.

Researchers estimate that infected PCs number in the hundreds of thousands. One must question the motives of the Sinit Project: some have been observed to distribute diallers (covert calling to expensive premium number services), but curiously, the potential for much broader abuse remains as yet untapped.

Conclusions and Predictions

The vast pool of insecure broadband PCs has come to be recognised as a valuable, free 'resource' and the plans of criminal gangs to commandeer these are well- progressed, as a platform for a range illegal activities. Criminal agendas are set to expand even further in 2004. Extrapolating existing trends, **spam, worms, trojans, spyware, phishing and distributed denial-of-service attacks will escalate in 2004. Despite arrests, identity theft, ebank robbery and protection rackets will continue to increase.**

A devious cyber-criminal, operating through a complex chain of proxies, can conceal the point of origin very effectively. However, grammatical characteristics (in spam, social engineering associated with worms, and phishing) can provide useful clues to the general origin of an author, for whom English is a second language. Furthermore, sloppy selection of locations for fake ebank web sites can betray the location of the criminals. Offers of spam services for hire are traceable. Finally, the most effective investigative routes involve following the money, in attempted money laundering and protection racket demands. Consistently, the majority of the clues point to Russian and East European sources.

Any group participating in cyber-crime alone can remain well-hidden, despite revealing the country of origin. Mafia, however, who are also dealing in drugs, prostitution, arms etc. are rendered relatively visible as a consequence and **arrests will be announced early in 2004**.

Does the abject failure of Sobig.F to hijack any PCs in August and the absence, so far, of a G version, mean the project has been abandoned? That would seem unlikely, as with a few refinements, F could have been enormously successful. Unless the perpetrators are apprehended, **it is likely that, in 2004, Sobig.G, with a throttled back mass-mailing and many second stage locations may prove decisive.** Much depends on optimised timing of the second stage: long enough to allow wide propagation, but short enough to win in the race to close the sites down.

The emergence of the Sinit P2P trojan network is intriguing. Not only does this represent a major milestone in the evolution of malware, but also it could constitute the launch pad for a highly efficient 'Superworm'. Theorists have postulated the 'Warhol' and 'Flash' superworms, capable of infecting all vulnerable hosts on the Internet in minutes. The optimal pre-infection strategy, dubbed 'Curious Yellow', proposes a cooperative network of worms gathering a list of vulnerable targets and then sharing the infection task, such that any target will be infected from one source only. The Sinit P2P network could provide just such a base. Much depends on the motives and ambitions of the owners of the network. So far there is little evidence to suggest that their primary intent is financial gain.

Sinit may not be the only candidate for the next Superworm platform. Low profile scanning of the entire Internet has been observed in 2003. Trojans have been released in unprecedented numbers in the last six months - to what purpose? Some have speculated that some of these trojans, although appearing to be malfunctional, may be interworking in a very stealthy manner. If so, this suggests a scanning exercise, as a prelude to the release of a new Superworm. Unlike, Slammer and Blaster, which served no objective beyond rapid spreading, **the next Superworm in 2004 will probably execute a power grab for control of all vulnerable hosts available on the Internet.** As a global resource, this represents a much bigger prize than the base of home broadband PCs hijacked in 2003.

How far can matters deteriorate before they become intolerable? It is conceivable that **2004 may see consensual agreement to the introduction of radical regulatory measures**, as espoused by Eugene Kaspersky. At the very least, further deterioration should hopefully engender **closer collaboration between 'White Hat' hackers, antivirus researchers, law enforcement and Internet Service Providers**. We are singularly ill-prepared to face the challenges 2004 could pose and may need to mount some kind of international defence force to meet them.

Practical Protective Measures

Antivirus protection is an essential element, but employing reactive measures has become increasingly marginal, as the time to apply updates can easily exceed spreading times of worms and trojans. Pro-active countermeasures assume greater importance.

Individuals, with home PCs, unwittingly sit in the centre of the new battlefield and must take steps to safeguard their systems against infiltration:

- Disable File and Printer Sharing for Microsoft Networks, on your network and dial-up connection settings- this exposes you to attacks from the Internet
- Delete any email with attachments, unless expected or explicitly confirmed as 'bona fide', from a trusted source.
- Harden the Achilles Heel of Windows systems - Internet Explorer - by means of Quik-Fix, available from one the foremost security experts in this area http://www.qwik-fix.net It will protect against known (but unpatched by Microsoft) and future unknown IE problems that may allow trojans and spyware to infiltrate your system, either from email or malicious web pages.
- All virus, trojan and spyware infiltration will result in predictable modification of certain Registry keys, so as to allow the invader to run, whenever Windows is rebooted. Disallow any attempt to write to these crucial registry keys (unless you are in the process of installing legitimate software) by installing a monitoring program such as RegistryProt free from DiamondCS http://www.diamondcs.com.au/index.php?page=regprot
- Install a personal firewall or enable Windows XP's built-in firewall.

Organisations cannot rely on a simple combination of firewalls and antivirus and need to apply security-in-depth, including the following important steps:

- Apply email content filtering software e.g. CS MAILsweeper™ for SMTP. Block, as a matter of routine, all email with executable filetype attachments, including at least .COM, .BAT, .PIF, .EXE, .CMD and .SCR. http://www.clearswift.com/products/msw/smtp/default.aspx
- Apply web content filtering e.g. CS MIMEsweeper™ for Web http://www.clearswift.com/products/msw/msw_web/default.aspx
- Combat the deluge of spam with CS MAILsweeper™ Anti-spam Solution http://www.clearswift.com/products/msw/antispam/default.aspx
- Apply Microsoft patches, in a timely fashion.
- Harden all laptops (as described above for home PCs): these provide easy access routes into otherwise well-protected networks.

Finally, Internet Service Providers are uniquely placed to intervene as reinforcements in this battle by:

- Blocking all upstream servers in their broadband population that have not been officially requested by the customer.
- Offering value-added services, such as periodic port scans to pinpoint exposures in their customers' defences.

2003 was the worst year on record for malware, but 2004 promises to be a real roller-coaster. Good luck for a happy New Year.

CLEARSWIFT™

Managing and securing
electronic communications

EUROPE

United Kingdom
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany
Amsinckstrasse 67
20097 Hamburg
GERMANY
Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

France
54-56 Avenue Hoche
75008, Paris
FRANCE
Tel: +33 1 56 60 58 00
Fax: +33 1 56 60 56 00

Sweden
Skeppsbron 16
111 30
Stockholm
SWEDEN
Tel : +46 708 89 0001
Fax : +46 8 21 78 10

AMERICA

US West Coast
15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: +1 425 460 6185

US East Coast
1050 Winter Street
Suite 1000
Waltham
Massachusetts, 02451
UNITED STATES
Tel: +1 781 839 7321
Fax: +1 781 522 7488

ASIA PACIFIC/JAPAN

Australia
Ground Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel : +61 2 9424 1200
Fax : +61 2 9424 1201

Japan
Eisho Takanawadai Bldg 6F
2-11-8,
Minato-ku Shiroganedai
Tokyo-to, 108-0071
JAPAN
Tel : +81 (3) 5423 8171
Fax : +81 (3) 5423 1274

www.clearswift.com