Responding to Internet Threats - Worrying new trends

Recent research from several sources has highlighted some rather worrying new trends.

Those following the evolution of security threats over the last few years will be aware that significant risks to an organisation's security are no longer just those posed by traditional viruses carried via email. More recent concerns surround the increased downloading of malicious objects through browsing of infected websites. The purpose of malware transmission has also changed in this period, from vandalism (those wishing to cause annoyance or destruction of computer systems) to stealing data for monetary gain by sophisticated fraud or simple theft.

Worryingly, the most recent emerging trend is that the websites that are infected with malicious payloads include a significant proportion of sites with good reputations. Network Managers and no doubt ordinary users have been wary of visiting, shall we say sites of dubious reputation, at least during working hours for obvious reasons. Not only do they deliver questionable content but are well known to deliver spyware and malware of various types. Surprisingly, researchers have found that between 75% and 80% of malicious code browsing infections are now being delivered by legitimate sites that have been compromised. If these statistics are correct – this is a highly unwelcome development.

So what are Network Managers to do? We discuss this topic in greater detail and suggest some procedures that can be adopted in your organisation and describe what can be implemented on your NetPilot to further protect your organisation.

The Financial Dilemma

The unfortunate situation that organisations find themselves in, particularly in today's financial climate, is that IT security risks continue to escalate, while budgets possibly stay the same or decline. Things are further complicated and resources spread more thinly, with evermore members of staff becoming mobile, no longer just working from a single PC at a desk at an office location.

Recent campaigns by those supporting WikiLeaks has shown some major banking and credit card organisations, who undeniably spend big bucks on all elements of IT security were found wanting in combating denial of service attacks. Quite how thousands of activists all downloaded the same simple tool (which laughably did not anonymise the users' source addresses), were able to significantly disrupt the operations of these financial companies is definitely surprising, if not disturbing for end-user customers of such organisations such as you and I. While large budgets do help, spending reasonable amounts countering the obvious threats to your type of organisation, with adequate processes, procedures and countermeasures is essential.

The author of this paper has seen first-hand where a company recently decided to follow an ill advised cost cutting policy and reduce spending on what appeared to be overly expensive IT security. The end result was to implement no effective security. The organisation's online ordering system was quickly compromised leading to disclosure of numerous customers' credit card details to criminals. Unsurprisingly, the company in question is loath to go public on its actions.

Where are threats really coming from?

Recent research has shown that searching for something as seemingly innocuous as entertainment or news often leads to users being presented with links to malicious sites. These techniques are called Search Engine Optimisation (SEO) poisoning. When for example, a big news story occurs (sporting, natural disaster, political or whatever), criminals manipulate the results given by search engines such as Google. High up the list of links presented in answer to the requested search, are links to sites which have been artificially promoted and once followed, provide scammers with all sorts of opportunities. Hence users are just one click away from a potential security threat from just searching for a football result!

Email does not seem to capture the headlines it once did as a potential area of threat (or 'threat vector' as some would term it). However, with between 85% and 95% of all emails - depending on which research you read - being spam, there is still a high likelihood that a significant percentage don't want to sell you something, but would rather steal something from you.

Those selling you internet security solutions like to highlight 'Blended Threats' as being the big thing to counter; so what are these? The best known example is 'phishing'. As everyone will be aware you are sent an email allegedly from someone or some organisation you know well and are then are pushed to use links within the email. Attempts are then made to extract various financial details from you or your PC. Despite security vendors saying blended threats are becoming more sophisticated – some of the simpler things seem to work best for the scammers.

Recent simple scam examples include emails or website content urging you to use or download Registry Scanners or Anti-Malware tools. Their intended purpose is definitely to scan your PC, but for criminal purposes and definitely not to aid you to defeat any hostile software. 'Drive-by Downloads' are another example of a somewhat more straightforward approach to getting unrestricted access to someone's PC. These downloads are sometimes actually authorised by users who just don't understand the consequences of saying "yes" and other times ActiveX, Java or executable programs are just stealthily downloaded.

Social Networks are a superb information resource for scammers intent on identity fraud or other criminal activity. Part of the so-called Web 2.0 wave (of advances over the original web?), these websites make incredible amounts of information freely available, often building unjustified levels of trust from 'friends' in a community. The likes of Facebook, Twitter and blogs are highly targeted – precisely because they are used by so many people. Criminals take advantage of users' openness and willingness to share information.

But what to make of increasing use of Twitter and Facebook by companies? Some are plainly in businesses where they are selling to consumers whose profile fits the average user of these social networks; hence it makes perfect business sense. Many others have flirted with a presence on these types of networks – but do these websites make any sense for the majority; or they are just following the fashion? In another survey between 10% and 30% of employees stated they absolutely needed access to these social networks for work purposes. Perhaps the marketing department needs access, but does anyone else in the organisation really need 'business' access?

While the worm attacks on Twitter and Facebook have been well documented and the disclosure of personal information on these sites are obvious avenues for criminals to exploit, blogs on the face of it, seem more innocuous. However there are 15 million blogs out there all using Wordpress. Most of these are using out of date versions and are easily compromised. With updates (security and other) happening just three or four times a year from the WordPress developers, this software is not what anyone would call robustly secure.

Another long time fact of life is that unless kept fully patched and updated, Microsoft software is unusually susceptible to being compromised; not because of poor craftsmanship on behalf of Microsoft's coders, but rather as it is the de facto standard software in many arenas. It is therefore the starting place for any hacker. This goes for versions of Internet Explorer browsers, through to webserver software such as IIS, through to operating systems for PCs and servers alike. It's remarkable that with so many known exploits of older browsers such as IE6, that one will find many visitors to any website still utilising such ancient and easily compromised browsers.

Successfully Surviving Multiple Threats: Top Marks in Education

Take the average secondary state school. Its Network Manager has to contend with six hundred to eight hundred PCs, 4 or 5 servers, a hundred teaching staff who usually aren't very IT literate, plus a thousand or more other users (also known as students), who are very IT literate and would definitely delight in breaking his network. Often the Network Manager has only one or two network staff to assist. So in terms of network size and numbers of hostile users - his task is typically much bigger in scale than most commercial counterparts.

As internet access is now mission critical to teaching, having an operational network and one that does not allow access to undesirable and illegal websites is absolutely mandatory; as is blocking of anyone external trying to get into the school network for whatever dubious reason.

This is also a political environment, where the Network Manger is in a no win situation. If network security or availability is poor or broken, it's his fault. If staff members lose files it's his fault. If little Wayne's father is complaining to the school governors that his son can browse pornographic sites from school PCs – again it's his fault. So undoubtedly there are also multiple threat vectors to the Network Manager's job security!

To survive these multiple threats school Network Managers do the simple things well and don't trust to luck or good judgement by users. Some of this involves developing simple processes. Some of this involves policing and protecting by technology. In short it's devising a ***'Security Survival Plan'***, which often includes the following action items:

- If possible, put users in a 'Walled Garden' internet filtering group – only allow them to see a restricted set of sites. This blocks both undesirable content and the likelihood of downloading malware. The allowed sitelist may contain several hundred or even thousands of sites – but these are all of known reputation. This is much more effective than any blocklist.

- Block all illegal and undesirable sites for everyone including staff. Overblock rather than underblock.

- Lock down PCs using low cost but effective software designed for the job (onetime costs of about £5/PC), so no hostile user or malware can take out a workstation – regardless of the Microsoft patch status.

- Teaching staff will undoubtedly want to visit non-work related internet sites for online shopping and booking holiday travel. Put the most popular and reputable sites into an allow list thus aiding protection against malware. Insist they use PCs that are locked down if they want totally free ranging access.

- Pupils will want/expect access to Bebo and Facebook. Some schools will want to provide this access at lunchtimes. As long as allow/block timebands are in place on the internet gateway device (to prevent access during 'working hours') and access is being undertaken from locked down PCs, this is an acceptable compromise.

- If possible adopt a belt and bracers approach to scanning for malware. Load each laptop and desktop with market leading AV software, but also undertake scanning on the incoming internet feed. Sometimes maybe this is undertaken upstream in the education network, if not implement a different AV and Anti-Malware scanner at the school gateway.

- Have in place Acceptable Use Policies (AUPs). Put into simple words, simple protection measures that both staff members and pupils will understand and have to literally sign-up to. If you need to take sanctions against hostile users, you need to have the legal groundwork in place. Such policies also spell out obvious security measures to staff laptops - don't download software and don't mess with AV or other security settings.

Interestingly, a number of schools use NetPilot products on which to implement key elements of their Survival Plan. So there are some obvious points to learn from the education sector and implement in the business world, as discussed below.

Responding to Internet Threats in Small and Medium sized Businesses (SMBs)
New Year's Resolutions for Network Managers - 'No More Head in the Sand!'

As recently published statistics have shown, the internet world has changed and continues to change. This requires corresponding changes in attitudes regarding employee internet access and IT use. This can perhaps be characterised as a change to a more realistic security policy, from a previous 'head in the sand – I see no issues' approach. At the beginning of a New Year, it's the ideal time to put an ***Action Plan*** in place and can be one New Year's resolution you should keep!

Without being overly dramatic, because the company network is attached to the internet, this has potential to severely impact the company financially – as even large companies have found recently. Employees can update their Facebook profiles, book their holidays and make online purchases at home. Why offer them the opportunity at work where the by-product might be to compromise the business network and impact the business itself?

Many commercial organisations, especially smaller companies, operate on the 'trust' principle that their staff will not waste time and resources by 'playing' on the internet during working hours. Even if this trust is well founded – the likelihood of staff with free reign unwittingly downloading malware is extremely high. Monitoring internet usage is often an eye opener - seeing how much non-work related activity is actually being conducted. The fact that staff dipping in and out of Facebook during the day is not only a time waster, but also a security and resources issue hasn't occurred to many SMB managers or business owners as a big issue.

The company resources are installed for business use; the company and its security in all senses has to come first. The Network Manager and more importantly his senior management have to put company security at the top of the agenda.

For those that hesitate over the need for such action – two interesting questions:

- **Q:** How do you know that your network and/or company website hasn't already been secretly compromised?
  A: Possibly you don't. Worse, you may not be able to legally demonstrate that you have 'adequate and reasonable' measures in place to protect your customers and staff which you are obliged to undertake.

- **Q:** Could you be legally liable when staff using your business network for private banking purposes for example, have their funds and/or identity stolen?
  A: Yes. If you cannot demonstrate you have put 'adequate and reasonable' protection in place. So why get into this dilemma by allowing such non-business activity?

Drawing heavily on the education example above here are some simple suggestions for SME network managers – particularly those that have access to NetPilot equipment or are considering purchasing in the future.

Action Plan - Summary

- *Create and publish a company Acceptable Use Policy (AUP).*
  This sounds a boringly formal place to start – but it is essential.

- *Implement and enforce a Security Survival Plan (SSP).*
  This is a combination of processes and technology configuration. This is the next step on from your AUP.

- *Monitor and amend your AUP and SSP.*
  Again use of technology to help amend the processes and modify written documents.

Action Plan - Detail

1. Acceptable Use Policy for SMBs

Without an AUP in place the organisation has no legal and practical framework. It has far more restricted room for manoeuvre if (in extreme situations) it needs to take sanctions against an employee. The AUP ensures that all parties are agreed that the company has the right to monitor and control use of its own network.

Your AUP needs to be simple and to the point and importantly sold to employees. They need to understand the reasoning and sign-up (literally) to a process that the company is implementing to protect itself from internet risk and fraud – and importantly indirectly protect their employment. The AUP emphasises to employees that the company internet access and network resources are in place for business use.

The AUP needs to evolve over time but we have included a straightforward template devised by government funded Businesslink.gov.uk. Alternative and potentially more complex AUPs are available online from solicitors and others but will undoubtedly need amending for your own environment.

2. SMB Security Survival Plan

Again keep it simple and achievable.

- Block all illegal and undesirable sites for everyone. Overblock rather than underblock.

- Emphasise in your AUP that the downloading and installation of non-approved software on employees' company owned PCs and laptops is forbidden on security grounds. If necessary block certain file types such as executable program files to discourage this practice.

- If possible, put all or most users into a NetPilot whitelist internet filtering group. Only allow them to see a restricted set of sites they need for business use. Importantly, this blocks both undesirable content and the likelihood of downloading malware. Significantly it also stops time wasting. For many organisations this whitelist may contain only a few dozen or a few hundred business-related sites – but these will be of known reputation and less likely to have been compromised.

- Certain departments or individuals will claim that general restrictive whitelists make their work related tasks impossible. For these staff members implement either a customised, more open whitelist, or restrictive blocklists. Point out the AUP restrictions on downloading non-approved software.

- Staff will undoubtedly want to visit non-work related internet sites. The employer may feel 'obliged' for one reason or another, to provide these facilities. If this is the case, install separate 'locked down' PC(s) on the DMZ of your NetPilot and implement a less restrictive blocklist for these devices with access times controlled by NetPilot timebands. 'Locking down' can be achieved using cheap but effective software, providing a defence against malware or users downloading questionable software, either deliberately or inadvertently.

- Adopt a belt and bracers approach to malware scanning. Load each laptop and desktop with market leading AV software, but also undertake scanning on the incoming internet feed at the gateway NetPilot.

- Update all old browsers. Put in place plans to ensure all PCs and Servers are running sufficiently patched software. Ensure you have enough time to conduct regular audits and updates.

- NetPilot can really help with securing remote communications from mobile devices or branch offices. Using ultra efficient encrypted SSL VPN tunnels and Data Leakage Prevention software (enhancements added to NetPilot V6 software in the last 12 months), could be a major help in improving both network security and performance.

- Medium or Longer Term. Look at ways of using Thin Client PCs – devices that are implicitly locked down with no ability to be compromised. This goes hand in hand with thoughts of using more centralised private or public cloud services where computing is centralised. Admittedly cloud technologies introduce the prospective of differing security threats. However, NetPilot has introduced its 'Cloud Ready – Cloud Safe' program to assist in this respect.

3. Monitor and Amend AUP and SSP policies and documents

These are living entities which will necessarily evolve over time.

- Keep your AUP updates and published on your intranet or equivalent.

- Keep staff appraised of (and sold on) successes and modifications needed.

- Use NetPilot logs and analysis functions to improve or modify whitelists and blocklists.