

the device has been retrieved. DGI has conducted a number of successful investigations using this method. The memory on these devices is substantial – so much so that the target's activity at the computer may be monitored for months and even years. In the last year DGI encountered one specific instance where key-logging devices had been used offensively to snoop on specific computer users within a major commercial organization.

Other methods employed to snoop on computers include the remote installation of embedded programs such as 'Back Orifice' developed by the self-styled hacker group 'The Cult of the Dead Cow'. Back Orifice enables the snooper to administer and control a PC remotely. Obviously, email is also open to abuse. DGI has investigated numerous cases of private and confidential electronic mails being routed to unauthorized users without the knowledge or consent of the intended recipients.

Paradoxically, computer technology is getting both larger and smaller simultaneously. The data storage capacity increases as the physical size of the storage and processing devices decreases. Memory sticks, roughly the size of a small box of matches or a lipstick, with up to 512 megabytes of

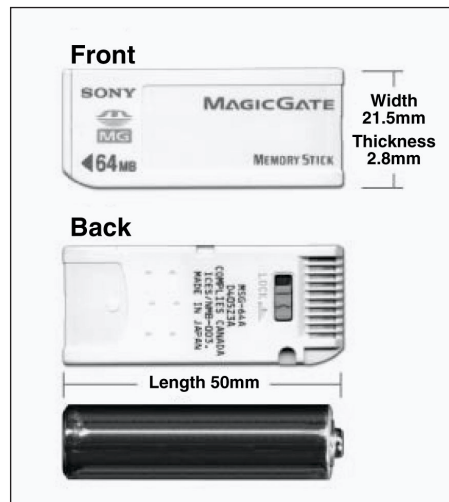


Figure 2. A memory stick. This model from Sony stores 64 megabytes of data — approximately the equivalent of 44 high-density diskettes.

storage capacity, can be purchased for a few hundred dollars. Available, also, are fully functioning wristwatches capable of storing 256 megabytes of data, downloadable using a standard USB 1.1 port. Understandably, these and similar developments, not least solid state storage for digital cameras, have caused some major revisions in the training of law enforcement officers in search and seizure procedures.

This technology is now at the disposal of the skilled investigator but it naturally follows that it can equally be used by criminals and others to misappropriate information, or to aid and abet fraud and computer misuse.

As previously reported in *Computer Fraud & Security*, DGI noted that the single most prevalent computer misuse in the year 2002-3 was the theft of intellectual property and proprietary data by trusted insiders. I predict that we will see a commensurate increase in data misappropriation by outsiders, professional snoopers and amateur hackers alike, given the plethora of tools now at their disposal.

To conclude, it has never been easier to snoop on you and your organization, or steal your data, than it is now. You have been warned.

References

¹To reduce background noise or clutter and enhance the clarity of a recorded conversation.

Data Genetics International Limited
London WC2N 6AA

Direct: +44 (0)20 7520 9386/7

www.dgiforensic.com

Email and Web Abuse — Monitoring & Investigations: Part II

Matthew Pemble

Web monitoring

With the Web, there is a little more preventative work that can be done to prevent abuse than with email. URL filters, although I fundamentally oppose them from an engineering design point-of-view¹, are a necessary and unpleasant evil in the corporate world. They can prevent the vast majority of the innocent and casual browsing of offensive and similar material, although the dedicated seeker after pornography will always be able to find sites that have not yet been picked up by the filter database team.

Most of the really offensive material moves quite regularly, either to prevent it being taken offline by law enforcement or, for the more blatant, after being taken actually offline.² Added to that, the really dedicated pr0n barons can easily set up a remote SSL proxy and navigate that way. The committed, especially away from Head Office, could, with a bit of help from IT, set up a special proxy within your infrastructure to allow them to browse at will. I have heard of cases where this has happened, not looking for pr0n, but to allow people to access gambling and gaming sites.

Now, given that you have the blocks in place, what can you do? Well, you could watch the reports from the blocking system – but that isn't too great a solution. I bounce off the corporate blocking system

on a daily basis, mostly hitting ebay.co.uk as a result of geographically targeted Web-page pop-ups³. People whose job actually involves surfing as a major part of their employment are going to run into these obstacles on a regular basis⁴, and may overwhelm the system with innocent false-positives⁵. This is likely to render nugatory most such endeavours, as well as potentially providing a huge privacy problem with this as an aspect of monitoring rather than investigations. Remember that few people are going to have a full and proper idea of exactly what is blocked by your particular filter and, therefore, innocent recreational surfing may reveal sensitive private details of personal lives. As a trivial example, consider what might be made of a person googling for information about venereal disease, followed by a search on the local health service site for the closest VD clinic?

A useful alternative is a second monitoring and reporting system, using keyword detection but not conducting any blocking. This does not have the same power to protect staff as site blocking and should be considered as a secondary control, in most cases. Remember that every block you implement has a chance of impacting on legitimate work, including fraud investigations and customer complaint handling, therefore you will need to consider bypass routines, which will be addressed in the investigations section.

Investigations & evidence

Oversight

Once you have identified suspicious events, it is necessary to initiate an in-depth investigation. At this point, a formal procedure, agreed with your human resources department, is essential. If possible, the input from the monitoring function should be used to conduct an initial risk analysis, to see whether the necessary intensive resources should be committed. Any such decision ought to be made by a trained and experienced manager, working from a fully documented and approved set of criteria.

Obviously, certain circumstances are going to make it vital that some degree of investigation is conducted: illegal activity, racial or sexual harassment, or formal complaint of objectionable behaviour. In many cases, the inevitable resource constraints are likely to mean that you would not be able to conduct an efficient and comprehensive investigation, therefore concentrating on those events most likely to cause a serious problem for your organization. As with many categories of incident, different organizations will have different priorities and different potential sanctions, including administrative “penalties” such as the removal of Internet access privileges.

Any investigation will need to be conducted under proper authority and supervision, using high-privilege network accounts. I most strongly recommend that investigators have separate, comprehensively audited accounts specifically for investigations purposes, rather than having increased privileges on their day-to-day accounts. An authorization system, with defined parameters and responsibilities, will give a degree of control over the investigations process. One of the more serious problems with any form of investigations team is to make sure that they keep emphatically within the boundaries of the established and approved policies.

One of the more critical decisions to take is what degree of investigation is necessary. In some cases, especially complex frauds, recovery from backup tapes, forensic analysis of workstations and laptops, and detailed analysis of all business contacts and transactions may be justified. In simple email misuse cases, a simple list of the titles and recipients of emails sent during the last week may suffice. The requirements for the degree of “evidence” required will depend on the nature of the misconduct – breaches of corporate policy are unlikely to require the same meticulous analysis as a criminal act that may end up with law enforcement becoming involved. However, it is useful always to treat cases as if they may end up in some form of legal action (including Employment Tribunals, or the local equivalent) and maintaining records sufficient to meet the standards involved.

Facilities

Your investigations team are going to require some moderately specialised facilities, seemingly archaic in the modern open-plan, “all in the same team” world:

- Firstly, you need a secure office with a number of workstations that cannot be overlooked from outside.
- Secure storage, including storage sufficient to meet local chain of custody regulations, is essential.
- A number of “dirty” computers, to be used specifically for offensive material investigations.
- High-speed printing facilities, within the closed office.
- Secure document disposal.
- Computer forensics capability (could be an external contract.).

Access to a dedicated and well-trained human resources team is also vital. The nature of much of the material produced in investigations is sufficiently offensive that it is only fair and reasonable that everybody who has to deal with it is assessed and briefed prior to their initial encounter with this genre of activity. I specifically ask, in interview for investigations and related positions, what attitude potential staff would have towards paedophile material. You cannot, and should not, exclude a candidate for their opinion on this, however it is necessary to ensure that investigations staff have the necessary objectivity and professionalism to approach even the most appalling cases from the attitude of proving the events, rather than the old military tradition of “wheel⁶ the guilty guy in.”

Another significant issue is the required access to inappropriate websites or, even, to blocked IP protocols and services. It is not acceptable to break security to prove security – your organization has spent large sums of money to establish a relatively secure network perimeter. It is fundamental that the fewer holes punched in to this perimeter, the better the absolute level of security. There are valid business reasons, in a large enough organization, for almost any activity, however the method of providing these exceptional facilities does need to be carefully considered.

Where straightforward protocols are involved, and the material intended for access is not objectionable within both (not either) the mores of the team and the more general acceptability to over-looking post-room staff, cleaners, and pot-plant resuscitation technicians. My recommendation is for a small number of very tightly access controlled standalone machines, in secure or semi-secure areas, that are not capable of being readily over-looked. Tight audit controls on access to and use of these machines needs to be implemented, with independent assurance that these are not being abused to allow access without that minimally necessary for the collection of evidence.

What constitutes evidence?

In the investigation, the team are going to have to consider two entirely separate issues regarding each suspicious event: what and why. Firstly, you need to establish what occurred – did, for example, pornography appear in a browser window on the suspect computer, who was logged in at the time and, in these days of Web bugs, Web bombs and other oddities, would a normal (i.e. not a security professional) user know that this had happened? Secondly, you need to work out why.

This is hard. As previously indicated, I watch a lot of **pr0n** at work. Not, unfortunately, because it is tasteful erotica, but because other people insist on downloading it from the Internet. This is a fairly blatant excuse: other members of staff will have jobs “skirting the edges of decency” – looking at customer or potential customer websites,

Email is, I have to say, relatively easy. You have no control over what you are sent. You have, if your system is behaving normally, reasonable control over what you send. Intent, in this case, is moderately easy to track down, at least to a user account. Proving, at the weight of probability or, worse, beyond reasonable doubt, that a specific human is connected to account activity is, in the Chinese sense, “interesting.” That, thankfully, is the subject matter for a future excursion.

Web is also, variously interesting. Even though you, normally⁷, have to enter a URL to go to a website, there are plenty of ways of making “stuff” appear on your browser that you didn’t actually attend. Mistyped URLs, redirects, hijacked domains, dodgy adverts on otherwise legitimate sites and many other weird and wonderful methods of pushing rubbish on to your screen (often twenty or thirty windows at one time, nowadays), mean that you need to be very careful in ascribing intent to rubbish appearing in suspects’ Internet histories. Actually, you need to be very careful in ascribing individuals to computers’ Internet histories. Careful time tracking, a good deal of suspicion and careful consideration is necessary when trying to work out exactly how much of what appears to be a concerted attempt to get as much explicit pornography on a computer as possible is actually intentional rather than just an unpleasant and miserable accident.⁸

You do need to carefully consider the quality of the material available to you, noting that in each case, the quality of every record may differ:

- Evidential – the highest grade of material, capable of admissibility into criminal court. Adherence to the UK ACPO standards and chain of custody is vital.
- Sub-Evidential – there is a considerable body of material that would not be admissible in a criminal case, but would be acceptable in many other cases, including Employment Tribunals.
- Indicative – Records that show that event has occurred but are not initially recorded with any measure of integrity. “Email chains”, where the previous “from” and “to” fields are probably correct but could be trivially forged.
- Formal – a statement made regarding an event: e.g. a complaint of harassment.
- Hearsay – comment with little or no evidential value.

Each record can be obtained from standard logging or from special investigations tools. Special tools are likely to

incorporate digital signatures, hashing algorithms or other methods of confirming the integrity of evidence. For records extracted from more normal business practices, you will need to use one of the integrity tools at the moment of extraction into your evidence system. Taking the simplest example, a hashing algorithm, you should follow a process similar to this:

- If possible, take a hash of the evidence in its initial place of record. This is often, however, not practical, i.e. an email account on a Microsoft Exchange server, which needs to be extracted first. In many cases, you will be dealing here with a dynamic operational system, therefore this will not remain static throughout the investigations process.
- Copy the evidence to your investigations system and hash it again. This record will become your primary evidential copy and should not be directly altered.
- Copy the primary evidence to one or more working copies, as required. At this point, you are likely to change the evidence, therefore it is important to record exactly what you are doing so that the defence, or an independent expert, starting with a new copy of the primary record, can duplicate your working process and get exactly the same results.

Disciplinary & beyond

Haah, you can relax with a well earned coffee. Your job is now done. Actually, no it is not. Whatever you have managed to provide as an evidence pack has now been sent to your HR team, they have suspended the potential malefactor(s), and everything will move smoothly towards a final written warning or a dismissal.

It rarely works that way. Denial, counter-accusation, senior management exasperation, threats of lawyers; all are possible even in what appear to be the most simple cases. What can you do to ensure that you have the best chance of coming out of this with your integrity, if not your ego, intact?

Be prepared for counter-challenges. Wide and often inaccurate publicity is given to matters of security and investigations⁹ and, to my continued astonishment, otherwise educated and capable men and women continue to abuse electronic systems. Challenges in the internal disciplinary process can be quite convoluted. You are unlikely to be present to answer questions directly, and the presiding manager or panel are unlikely to have much experience of electronic evidence and the capabilities of your systems. If the matter gets to court or tribunal, you will have needed to ensure that a number of basic conditions are met, to limit the effectiveness of the three main areas of legal challenge; on the basis of admissibility, weight or interpretation. The following are simple guidelines:

- In the UK, ensure that you have a properly justified and documented monitoring impact assessment, and that the requirements of the Lawful Business Practice regulations are blatantly met.
- Your basic evidence collection should be forensically sound – collected under legally sound principles, of guaranteed integrity and processed according to repeatable procedures.
- You need to ensure that your investigations procedures are both documented and followed. Investigators should keep notebooks recording the steps they take – these can then be relied on in court to assist memory. Cases are often heard well over a year after the investigation has concluded.
- Train your staff in the law and in the procedures of court and tribunal.
- Have a comprehensive awareness of the wider organizational procedures and policies (disciplinary, harassment etc), so that you can be careful to ensure that the accused are treated fairly through the disciplinary process.

Working with human resources, it is also necessary to ensure that the outcomes of disciplinary actions subsequent to email and Web abuse investigations are fair and consistent. An event resulting in dismissal in one business unit should

result, in the absence of clear mitigating factors, in the same sanction in another business area. This is hardest to keep control of in large investigations or where senior staff are involved. Clearly, the business will need to consider the overall business impact, but deviations from your established norms will need to be justified and carefully documented. The consequent risk of adverse judgements, particularly at employment tribunal, and any ensuing bad publicity, will need to be considered and accepted by executive management.

Keeping your team sane

Okay, I'll show my personal prejudices here – it is probably not worth the bother. If you have selected your team carefully to achieve the necessary balance of professional competence and investigative experience, they are probably already too far-gone. However, you have got a responsibility to your investigations team to ensure that their working life is reasonable and fair.

Depending on your organization's HR practices, regular counselling may be a reasonable option, especially if your situation is unfortunate enough to require regular exposure to paedophile material. Proper management and senior management attention, formal and informal is important, as is a considered reward structure.

It is likely that there is a sufficient variety of casework that rotating individuals through different types of investigation will be relatively simple – complex frauds are much more interesting, for most investigators, and generally less unpleasant, than offensive material investigations.

The most important thing you can do is to build an effective team ethos: this will normally boost work rate, reduce the personal impact of investigations and build consistency in practices. Management need, however, to ensure that “team think” does not begin to dominate the necessary adherence to corporate policies.

Resources & further reading

There are numerous resources available for further research on this subject, never forgetting your friendly local employment lawyer. The following websites are recommended for viewing:

- The Information Commissioner's Office: www.dataprotection.gov.uk
- Version 3 of the ACPO Standard for Electronic Evidence will shortly be available from www.nhtcu.org
- UK legislation back to 1988: www.legislation.hmso.gov.uk/acts.htm
- Information on the UK Employment Tribunal systems: www.employmenttribunals.gov.uk
- Home of NetAnalysis: www.digital-detective.co.uk

Note: In between the completion of the first and second parts of this article, the Information Commissioner has released the issue version 1.0 of “The Employment Practices Data Protection Code: Part 3: Monitoring at Work.” The language has been considerably simplified and although, with the Supplementary Guidance, it now runs to 85 pages rather than the 47 pages of Draft 7, much of this appears due to formatting issues, especially an increase in font size. The primary requirements (to conduct an impact assessment before initiating monitoring and to inform those being monitored of what and why monitoring is in place) remain substantially identical to those in Draft 7.

References

- ¹ Okay, actually, I loathe them.
- ² It should be noted that a concerted and dedicated attempt to bypass the filtering mechanism needs to be considered as worthy of further investigation in its own right.
- ³ A current, and hopefully temporary pop-up (I have nothing against ebay), is some sort of strip poker site.
- ⁴ Actually, as person-in-charge of the pr0n investigations team, I regularly bounce off of all sorts of sites. Myself, and my investigations teams, normally appear

quite highly up the list, and duly report ourselves in to our management.

⁵ Real and accurate detections of blocked pages, but without the intent to download that is impossible detect with any current technology.

⁶ “Wheel” in this context, being a military drill movement: a left or right turn taken over a number of paces.

⁷ But see <http://www.getreading.co.uk/story.asp?intid=6541>

⁸ I would like, if you work regularly with

Internet Explorer users, to recommend a simple, effective and relatively cheap tool – Netanalysis, by Craig Wilson. Biased towards law enforcement, slightly simplistic towards the more complex filtering and analysis, but very capable.

⁹ Much of the media comment regarding the Information Commissioner Data Protection Code has been both superficial and has incorrectly assumed that the code has force of law.

About the author

Matthew Pemble is an experienced security architect, auditor and investigator. Having left the military for the purgatory of consultancy, he has finally escaped to run the Security Compliance team for a major international bank. Qualified as an engineer, penetration tester and forensic analyst, he is now in charge of a small team at putting in to practice many of the views expressed in these articles.

Patch Management

Alex Bakman, CEO of Ecora Software

Imagine this scenario. As a security manager for your organization, your responsibilities include analyzing and applying patches to all Windows servers across the enterprise. Your process is going to each machine and manually evaluating what patches are missing and installing the most critical security patches as soon as possible. How long does this take? One hour per server? Two hours? Maybe more? How many patches are critical? How often do you do it? And, how many servers do you have? It doesn't take long to do the math to realize that your battle may be a futile one to keep up with the most critical, let alone every, patch that's released.

Now, one day your organization falls victim to a denial-of-service attack caused by the most recent worm, much like the SQL Slammer worm that affected so many organizations worldwide earlier this year. Access to your most critical servers is unavailable, email is down, and worst of all business continuity at your organization is compromised. Your day just got even more stressful. And, then you learn that if the proper security patch, which had been available for months, had only been applied to all servers, your organization would have been safe from this attack. Now, your day just got a whole lot worse. The “we'll get to it when we can” attitude of patch management just escalated to become the most important IT issue of your organization's CIO. Unfortunately for your organization, it took an event like this for patch management to get noticed.

Lessons learned

According to data from the FBI and Carnegie Mellon University, more than 90% of all security breaches involve a software vulnerability caused by a missing patch that the IT department had prior knowledge of. In fact, the SQL Slammer worm could have been avoided if a patch that was available six months earlier had been applied. Just ask the Bank of America, US Department of Defense, and Department of Energy, among many others, about the pain it caused.

If IT departments know about these risks ahead of time, then why do these vulnerabilities exist? It's because the manual process of patching the thousands of workstations and servers in their environments is nearly impossible. The Gartner Group estimates IT managers now spend up to two hours every

day on managing patches. And, when Microsoft alone issues a new security patch about every fifth day, how can anyone keep up?

Intrusion detection and firewalls are not enough?

The SQL Slammer worm also proved that firewalls and intrusion detection systems are not enough to protect you. Hackers know where security vulnerabilities are, and whether they are attacking internally or externally they can wreak serious havoc.

You may ask yourself, “I have an intrusion detection system (IDS) and firewalls installed so doesn't that keep me safe from a hacker's attack.” While IDS and firewalls may keep a majority of external attacks at bay, a skilled hacker will still find his/her way in. And, don't forget about attacks generated from inside your organization. In today's slumping global economy with so many layoffs and disgruntled employees, internal attacks are on the rise and your IDS and firewalls are generally helpless in these situations.

Over the years, organizations have focused exclusively on keeping the bad out, but some of these recent publicized attacks have raised the awareness for the need to fortify internal systems. Patching systems can significantly reduce security vulnerabilities. A completely