Detect and Survive

By Robert Schifreen, UK-based IT Security Consultant and Author of *Defeating the Hacker*

Guidance® SOFTWARE
The World Leader in Digital Investigations™

1. SUMMARY

The ability to detect complex cases of computer misuse within an organisation, whether perpetrated by outsiders or from within, is vital to the continuing survival of the company. But as computer criminals refine their techniques, so must the detection methods evolve. To enable this, modern-day IT departments need to employ techniques and tools previously only available to forensic investigators within the law enforcement community. Thankfully, those tools are becoming available outside of the justice environment, and are proving highly effective in solving cases that would otherwise have remained impossible to close.

2. INTRODUCTION

The ability to examine the contents of a hard disk or other storage device at a very deep level has long been a fundamental requirement of technical support personnel and data recovery specialists. They need to analyze the data below the level of the operating system, on a per-byte or per-sector basis, rather than per-file. Those bytes or sectors often comprise current files, but this may not always be the case. Often, the data will represent remnants of deleted files, or information from the partition table, directory structure or other key elements of the copious metadata that exists on every hard disk, CD, DVD, USB pen drive, SD card, and similar devices.

Beyond even the requirements of support personnel and data recovery specialists is a level of device examination product known as forensic examination software.

3. FORENSIC EXAMINATION SOFTWARE AND LAW ENFORCEMENT AGENCIES

The need to forensically examine the content of a computer's data storage devices has always been important, but never more so than now. Criminals are using IT in all aspects of their lives. For example, no longer do terrorists keep lists of potential targets in notebooks – they store it in encrypted data files. Forensic examination of a seized PC can allow law enforcement agencies to recover that data, even if it has long since been deleted and/or the suspect denies that it ever existed at all.

The proliferation of Internet accessibility across the world has also resulted in the rise of another type of computer criminal, namely those involved in the creation or distribution of child pornography. The ability to forensically examine a suspect's PC allows prosecutors to steadily build a case as they uncover a series of small shreds of evidence, each of which may be insignificant when standing alone, but which helps immensely when taken together with everything else that has been discovered. For example, by uncovering fragments of deleted email log files, it's possible to find out which images have been sent from, or received by, the computer. By knowing which printers are, or have ever been, installed on a particular machine, the source of indecent photographs found in the possession of others can be positively identified and help to establish a link between suspects.

Of the companies which produce specialist forensic investigation software aimed at the law enforcement community, Guidance Software, and its EnCase Forensic product, stands out

as the most powerful and the best known. It's used by investigators and prosecutors across the world, and its reputation is second to none.

4. CYBER CRIME AND THE CORPORATE WORLD

The amount of computer crime, its financial and reputational impact on business, and the cost of recovering from attack, continues to increase despite the fact that almost every large company now has antivirus software, anti-spyware utilities, firewall, IDS and so on installed as standard. Clearly the corporate world needs to move up a gear in its efforts to defeat such activity and the people behind it. Criminals know that information and data has a tangible value, and will focus their attention on high-value targets such as credit card databases, e-commerce web applications, financial information, pharmaceutical intellectual property, energy and utility companies, retailers, government departments, telecoms operators and other high-profile organisations.

As companies large and small continue to fall victim to computer crimes perpetrated from both outside and within the organisation, corporate CERT (Computer Emergency Response Teams) groups involved in investigating breaches can no longer rely on traditional utility software, antivirus or anti-spyware tools to help them track down the cause of the intrusion and ensure that the damage has been cleaned up successfully. Such personnel now require the sophisticated forensic capabilities previously used only by law enforcement and criminal investigation specialists.

There is also an obvious requirement for that software to operate silently over a network. This is in marked contrast to the way in which forensic software has previously been utilised, whereby a computer is typically seized by police from a suspect and then taken securely off-site to be examined. In such an operation, the suspect is fully aware of the potential charges against him, and that his computer is to be forensically examined. While this state of affairs is acceptable, and indeed essential, within the law enforcement community and as part of a normal, fair judicial system, this is rarely the case in an ongoing internal corporate investigation into, for example, an employee suspected of leaking company secrets, stealing key data or making unauthorised use of the company's network. In such instances, the ability to covertly monitor the suspect's activity via the LAN, and also to monitor any other workstation or network device to which he attempts to connect, is essential.

Another example of this might be the case of a dishonest employee attempting to steal information from his manager's computer, and/or passing that data to an accomplice elsewhere in the company. Being able to have complete visibility into each workstation that is suspected of being involved, even if the user of that workstation is not suspected of any dishonesty whatsoever, is a powerful tool in the investigator's armoury.

Perhaps the greatest thorn in the side of IT security investigators right now is the increasing complexity and stealth exhibited by malware, which continues to increase in capability. Much of it is polymorphic, meaning that it continually modifies its own code to evade detection, and thus no two instances of the same program are sufficiently unique as to be identifiable by conventional signature-based scanners. Instead, detection is possible only by heuristics, (i.e. analyzing the behaviour of the code rather than its fingerprint) or by sophisticated data similarity detection techniques.

5. DETECTING AND REMEDIATING THREATS TO CORPORATE NETWORKS

EnCase Cybersecurity, from Guidance Software, is a product suite which provides CERT teams with the ability to detect and remove polymorphic malware, viruses, and other modern threats to the corporate IT infrastructure. Uniquely, it also includes key forensic investigation capabilities, based on EnCase Forensics, that provide the sophisticated tools that information security personnel need to detect and investigate unwanted actions on the network whether caused by rogue people, rogue software, or a combination of the two. EnCase Cybersecurity complements your existing perimeter security techniques, such as antivirus and antimalware precautions, by adding a new level of security. Malware which manages to penetrate your edge security defences no longer has free reign to go about its business unhindered on the network.

Because EnCase Cybersecurity is developed by the company behind the leading forensic software, it provides the unique ability to analyse the spread and behaviour of current threats, such as rootkits, at the kernel level. Guidance Software likens the product to the IT equivalent of an intelligent robotic scalpel.

To allow covert operation of EnCase Cybersecurity across the network, a small passive client application or "servlet" is installed on each workstation and server. This can be manually installed or rolled out centrally, with or without users' knowledge. The servlet communicates with the server-based Cybersecurity application, responding to the operator's commands to send back information about the workstation, such as the content of a particular disk sector or file. This allows the investigator or other trusted employee to home in on the source of a security breach or malware outbreak without the need to physically visit any of the PCs in question and, crucially, without alerting the user of that workstation to the fact that they are under investigation. It also means that, where no actual misuse is ultimately found, the innocent party remains untainted because colleagues will never be aware that he or she was ever under suspicion.

The servlet, and thus the features of EnCase Cybersecurity, is available for Windows, Mac, and Linux workstations, as well as Windows-based servers such as Microsoft Exchange.

The availability of a toolset to allow thorough covert investigation of all activity on the corporate network brings other benefits too. While most IT-literate consumers are all too aware of "Patch Tuesday", when Microsoft issues multiple security fixes for its operating systems each month, rollout of patches is often managed very differently within corporate environments, and for good reason. Many companies choose to run their own update servers, and only distribute patches to users' workstations after they have been extensively tested internally. Many patches and other important upgrades, such as new releases of Internet Explorer, are never pushed out because of conflicts with key internal applications, or because of the lack of available resources to re-train staff.

By not rolling out all important security updates to all workstations and servers immediately upon release by Microsoft and other application vendors, companies' networks are frequently less secure than admin staff like to think. Once a security patch is released, details on the vulnerability that it fixes are generally widely available. Hackers use this to track down and break into unpatched systems. Ironically, once safely inside, they sometimes install the missing patches in order to keep other hackers out.

One key feature of EnCase Cybersecurity is the ability to perform a targeted search for all important confidential files. Should these files ever find their way out of their normal habitat, either onto the public Internet or to unauthorised parts of the company network, this can be quickly identified. In the same way, EnCase Cybersecurity guards against polymorphic malware, as described above, by creating a profile that represents the expected state of any workstation or server during a typical day. If the system deviates from the expected, the unknowns are exposed for further investigation. EnCase Cybersecurity allows sysadmin staff to understand exactly where and how the organisation's confidential files are stored among the terabytes of unstructured data that exist within the typical corporate network, and gives them the means to remediate any unauthorised data transfer. By ensuring that confidential information is never where it's not supposed to be, the risk of data loss or theft is dramatically decreased.

EnCase Cybersecurity utilises multiple profiles, depending on what is being looked for. For example, there can be multiple workstation, server and even email server profiles, in order to ensure that unknown data can be highlighted no matter how it is introduced to the network. With this in place, any deviation from the norm becomes obvious, and can thus form the starting point of an investigation. The Bit 9 Global Software Registry, a database of more than six billion signatures of both known-good and known-bad files, has been completely integrated into EnCase Cybersecurity as part of this feature set. Any rogue program installed by a user on the network, or indeed any legitimate application installed without permission, can be quickly identified. And because this all takes place at kernel level, below the operating system, it works flawlessly on all workstations or servers, even those that have been compromised by rootkits or other low-level techniques that would defeat almost any other product available today.

In a typical proactive example, a company's IT security department might set up a scan to run overnight, scanning the network for instances of "crown jewels" files that aren't in their expected places—perhaps copies of the personnel database or as-yet-unpublished financial data on any workstation other than those of their owners. The scan takes place overnight, allowing the CERT team to subsequently act on the results the following morning in the so-called e-discovery phase, where the results of the scan can be analysed, put into context, and a course of action planned.

Additionally, the mere existence of such a system acts as a useful deterrent. Staff who are aware of the existence of such technology will be much more reluctant to misuse company IT resources.

6. CONCLUSION

Clearly, the benefit of being able to scan and forensically examine your entire network for evidence of malware, misappropriated files, rootkits, etc., provides a massive benefit, over and above that provided by traditional security techniques such as antivirus software and intrusion detection. It adds an entire extra layer of security to ensure that anything which penetrates your initial perimeter security does not have free rein. Thus, it can help ensure against the risks associated with an attack, such as the loss of reputation, not to mention legal penalties.

The days of having to worry about script-kiddie attacks on your network are no more. Today's e-criminals are sophisticated, skilled programmers. They know how to scan your network and evade your initial perimeter defences. Once inside, they have the skill to remain within your network. They'll destroy log files, or even install a hacked version of the OS kernel, in order to hide all evidence of their presence, or of their initial attempts to gain entry. These are known as APTs, or Advanced Persistent Threats. Once inside, these attackers are impossible to remove. Even if you tweak your perimeter security, by adding firewall rules or reconfiguring your intrusion detection system, it's too late. The Trojan horse is happy in his stable. He has no intention of bolting, whether or not you open the door for him.

To identify the source of such attacks, and eradicate them from the network, a corporate CERT team needs highly sophisticated tools at its disposal, and the skills to use them. Traditional disk examination software, and automated scanners, have a part to play, but the future lies in the ability to scan the entire network in-depth, and then perform forensic analysis on the results.

ABOUT GUIDANCE SOFTWARE (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by over half of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from Law Technology News, KMWorld, Government Security News, and Law Enforcement Technology.

For more information about Guidance Software, visit www.guidancesoftware.com.

WP 0130-50020