Featured in this issue:
The ABC of ransomware protection

Ransomware has become a significant problem and is now one of the most keenly recognised threats in the security landscape. And it’s likely to get worse.

Steven Furnell of the University of Plymouth and David Emm of Kaspersky Lab UK examine the history of ransomware and why it’s so effective. And they detail the steps individuals and organisations can take to defend themselves from this growing menace, including using anti-malware, back-ups and patching. Full story on page 5...

Exposing fraudulent digital images

We tend to believe what we see. But in the digital age, images are easily manipulated, and this can cause problems for fraud investigators.

David Spreadborough of Amped Software describes how images may be altered and the techniques we can use to spot pictures that have been modified. With the right tools and training, exposing doctored images in fraud investigations is now not only financially and technically viable, but urgently necessary. Full story on page 11...

Reinforcing your SME against cyber-threats

The small and medium-sized enterprise (SME) sector is colossal in terms of size and revenue. Given the critical role that SMEs play in the UK’s economy, breaches can have a major impact.

Keeping this in mind, Sneha Paul of ManageEngine presents six ways to reinforce your SME against cyberthreats. They include analysing logs, managing Active Directory, proactive surveillance, securing the cloud, password management and firewall analysis. Full story on page 13...

Data breaches: Deloitte suffers serious hit while more details emerge about Equifax and Yahoo

Deloitte, one of the world’s largest accountancy and management consultancy firms, has been hit by a breach that may have disclosed highly sensitive information about its customers.

According to a report in The Guardian, which broke the story, hackers gained access to Deloitte’s email system via an inadequately secured administrative account. This email system was hosted on Microsoft’s Azure cloud service and was first successfully attacked in October or November 2016. This meant the attackers had access to emails, potentially containing highly sensitive communications between Deloitte and its clients, as well as between Deloitte employees, for nearly a year. The admin account used just a simple password for authentication.

Deloitte, which provides auditing, tax consultancy and cyber-security services to banks, multinational enterprises and government agencies, has somewhat downplayed the story, issuing a statement that Continued on page 3...
This innate hardwiring means that the arrival of digital images has posed a problem for the fraud investigation community. There are many different reasons why someone would want to maliciously alter a photo to ‘tell a different story’. Although photos can be manipulated with ease, many people still harbour a natural tendency to trust photos as a true and accurate representation of the scene in front of us.

This innate trust in photos is engrained across all industries. Imagine the difficulty you would face by sketching your version of a contract with a pencil in a legal dispute, or submitting a painting as proof of a previously lost item when making a claim with an insurance company.

Digital manipulation

While this may sound a little extreme, photo manipulation techniques date back to the 19th century, almost as long as the history of photography itself. Modern digital manipulation tools have reached new levels of sophistication, with Photoshop now celebrating its 27th birthday. Such software can craft fantasies pixel by pixel, leaving the human eye none the wiser. Participants in a recent study could only spot irregularities in a doctored image 45% of the time.²

Even smartphone apps can alter images at the click of a button. Nowadays, children of primary school age can capture high-quality images, edit them and share with just a few finger swipes on their phones. It is easy to see how even minor changes can tell an entirely different story. For example, a quick rearrangement of words and letters on a document can change dates, statements and price quantities. Or the addition of just one face into a crowd scene creates an alibi out of thin air.

"Until now, many people have trusted the photographic image as being a true and accurate representation. This is evident in the news and media, where scandals of tampered images being ‘fake news’ run rife”

We cannot be so naive as to believe that fake images do not end up in fraud investigations. This is evident in the news and media, where scandals of
tampered images being ‘fake news’ run rife. We must ask ourselves the question, can we rely on this image we see before us? Has it been authenticated?

**Authentic images**

Luckily, image authentication procedures exist and take many forms in the digital forensic process. Image authentication has its roots in metadata analysis to identify and compare the hidden information in an image. Various options exist:

- Compression analysis to identify capture type.
- Visual analysis to identify signs of manipulation.
- Camera matching to link a specific device to an image.

Digital images therefore reveal their meaning and integrity not only by what they show but also through the metadata associated with them. The location data, for example, is embedded within the files and can be used to see if the metadata location matches what is shown in the picture. A suspicious document allegedly signed in London can be analysed to see if the metadata location verifies this.

Originally, this method of analysis required an extensive knowledge of a proprietary computer script and even a PhD in advanced mathematics to apply the algorithms required. Such techniques are promising but fall victim to an expertise bottleneck. They are ill-equipped to counter the sheer volume of consumer-friendly desktop and mobile phone photo manipulation freeware available at the click of a button.

But image authentication software has been catching up in the arms race against altered imagery. Modern software goes one step further and can use metadata to reverse image search online for other photos taken by a potentially stolen device. Each camera has a unique noise pattern from its sensor arrays and even two identical iPhone models will have a unique separate noise signature, analogous to a fingerprint. This makes it possible to track down and cross-compare online photos taken from a missing device using GPS metadata.

**Automating the process**

Software capable of automating the process of cross-comparing seized digital photos can piece together photos taken with the same camera and can build cases and link fraudulent activity to previously unconnected individuals. Information embedded in digital images can therefore help to protect individuals against criminal activities.

The need for non-metadata specialists to be able to quickly validate digital images is now more important than ever. Specialist software is used by police officers to authenticate images submitted as evidence in criminal investigations. Police officers undergo a short training course lasting several days and are then able to verify an image’s credentials without a PhD or extensive knowledge in coding languages.

“To effectively carry out fraud investigations in a world where anyone can edit and manipulate a photo at the touch of an app, we must remain vigilant and treat photo images with a pinch of salt”

It is not just scientists, academics or even police officers who should possess this ability as a base skill set. Journalists continue to battle with verification of fake news, a hot topic that understandably requires a more reliable means of detecting misleading images. Similarly, there is a need within the scientific community, where the need to verify questionable research paper findings is fast becoming a major issue. It is estimated that up to one in five published scientific papers contain imagery that has been tampered with.

**Remaining vigilant**

Image manipulation and image-to-camera identification is a unique and fascinating part of digital forensics that has growing importance. Seeing is no longer believing in this day and age. To effectively carry out fraud investigations in a world where anyone can edit and manipulate a photo at the touch of an app, we must remain vigilant and treat photo images with a pinch of salt.

The tools and resources are there to do this. A shift in attitude towards how we see photos and their merit in fraud investigation processes is vital. In the face of advanced fraudulent technology, we must urgently treat photos with the same level of suspicion as we would a drawing or painting. With the right
tools and training, exposing doctored images in fraud investigations is now not only financially and technically viable, but urgently necessary.

About the author

David Spreadborough is a forensic video expert at Amped Software (www.amped-software.com). Previously serving as a UK police officer for 24 years, he was a senior police officer within the UK Visual Forensic Unit and oversaw all major crime video investigations. Since working with Amped, he has provided a key role in the development of the company’s technical training, as well as spreading his passion for investigative reform through the latest technological innovations. Amped Software specialises in developing software solutions for image and video processing for forensic and investigative applications.

References


Reinforcing your SME against cyberthreats

Sneha Paul, ManageEngine

Despite its name, the small and medium-sized enterprise (SME) sector is colossal in terms of size and revenue. Defined as a business having less than 500 employees and either an annual turnover under £87m or a balance sheet under £75m, SMEs in the UK account for 47% of the private sector’s total annual turnover, at £1.8 trillion.1 Additionally, SMEs employ 15.7 million people, which is 63% of all private sector jobs.

Given the critical role that SMEs play in the UK’s economy, the scale and breadth of business is inconsequential to cybercriminals. Your organisation need not be a corporate goliath in order to be breached.

Safeguarding and defending against cyberthreats and attacks is imperative for every SME. A study by RSA says that SMEs in the UK are afflicted by a whopping seven million cybercrimes every year, with an average cost of £3,000 per incident.2 A cyber-security breach can spiral your budget out of control. Keeping this in mind, here are six ways to reinforce your SME against cyberthreats.

Audit and analyse log data

Log data is heterogeneous. It can come from varied sources such as network devices, Windows servers and workstations, databases, IP packets, applications and firewalls. While log caches are indispensable when it comes to troubleshooting an attack, careful log analysis is even more critical because it can help prevent attacks in the first place. Log monitoring and SIEM (security information and event management) solutions are essential in this case.

“You can strengthen your threat intelligence and include open source feeds to identify the global blacklist of IPs. This is accomplished using real-time reporting systems that send alerts via text or email”

Log monitoring software automates the process of auditing large amounts of data. It provides tell-tale signs of potential security gaps from a central console.

Generating compliance reports for SOX, GLBA, PCI DSS, HIPAA, FISMA and other regulations is also a lot easier using predefined or canned templates.

Furthermore, you can strengthen your threat intelligence and include open source feeds to identify the global blacklist of IPs. This is accomplished using real-time reporting systems that send alerts via text or email whenever a dubious IP is detected. Employing a solution to analyse log data is a great starting point to keep security vulnerabilities at bay.

Active Directory management

Internal threats loom as a big risk to corporate IT resources, with reports showing the percentage of insider attacks (combining malicious and inadvertent incidents) for the healthcare sector as high as 71%.3 Organisations have recognised that insider attacks (whether willful or