File integrity monitoring in the modern threat landscape


Mark Kedgley

Mark Kedgley, New Net Technologies

Anti-virus (AV) software, along with its firewall side-kick, has been the standard weapon against Internet-borne threats for the past two decades. But in a changing threat landscape, AV is fast beginning to look past its sell-by date.

Of course AV has a role to play in protecting businesses against the generic threat – the Internet vandal or hacker intent on causing maximum damage and gaining global attention. But such threats are now being pushed down the list of things that keep the IT professional awake at night, principally by the targeted attack – the stealth approach that can take months, even years, to slowly gain access to the most critical area of the business and remove data, leaving virtually no trace. Factor in polymorphous and mutating malware, delivered via phishing or social-engineered vectors, and AV is, quite frankly, useless against the contemporary Advanced Persistent Threat (APT). AV is not just fallible – it is fighting the wrong battle. It is time to wake up to new reality and implement a truly effective line of defence.

Slow and stealthy

Whether due to complacency or naivety, the vast majority of organisations have failed to adapt security processes and procedures to reflect the changing threat landscape. From the Chinese hackers gaining access to valuable intellectual property to the Russian gangs recently exposed for a $500m fraud, the attack model today is a world away from the loud-mouthed Internet vandal that used to dominate the headlines.

Today's attacks are carried out by groups, rather than individuals, are designed to steal valuable data and leave no trace. And these organisations are patient. A recent analysis of APT incidents by Mandiant revealed the average period over which the attackers controlled the victim's network was one year, with the longest almost five years. And these breaches are not just bypassing the AV software – growing numbers of APTs are actually inside jobs, with authorised users introducing keylogger software or malware directly to systems via USB devices. Throw in social engineering and irresistibly tempting phishing emails and there are simply too many ways to side-step traditional defences and infiltrate the business.

"A recent analysis of APT incidents by Mandiant revealed the average period over which the attackers controlled the victim's network was one year, with the longest almost five years"

Given the growing awareness of the trend towards the APT, why are so many organisations persisting on relying upon securing the perimeter solely via AV and firewalls – with many even acknowledging that the approach is probably 'secure enough'? It's not.

New reality

To be frank, AV was never enough, even in the days when the threat landscape was dominated by the attention-seeking big virus or malware creator. AV has to be updated daily in response to the new threats that have emerged – by default, during that time the business is at risk of infection. AV cannot address the zero-day, or zero-hour, threat until it has been identified, quarantined and an antidote created.

This model was flawed when the majority of viruses were noisy and high profile. In today's threat landscape, viruses and malware are the opposite – silent, stealthy and targeted. That means fewer organisations or individuals are affected – and hence there are fewer opportunities for the virus to be identified and neutralised. That zero-day threat might go undetected for some time because it is attacking a specific vulnerability within the business – or targeting a specific individual to gain access.

Mature model

If AV doesn't work – what is the option? First, organisations need to address the complacency that exists and start implementing some of the standard security processes and procedures that are key to defending the infrastructure and reducing the risk of compromise.

The recently unveiled draft standard 'Improving Critical Infrastructure Cybersecurity' has been produced by the US National Institute of Standards and Technology (NIST).[1] President Barack Obama's Executive Order 13636 recognised the need to legislate cyber-security measures in order to protect US critical infrastructure. The order mandated the need to share best practices and for NIST to provide a clear, cyber-security framework.

As a result of this fresh look at how best to defend against the contemporary cyber-security threats, NIST has produced a Framework Core, and within this a five-step methodology by which an organisation can assess risk and correspondingly protect information assets. The 'Identify, Protect, Detect, Respond, and Recover'

framework also places emphasis on the need for contingency planning so that, if the unthinkable happens and a breach is successful, the organisation can recover.

"The back-stop to traditional defences ideally needs to be a real-time alert triggered by any change to file structure that might indicate compromise"

Even so, in common with all other previous best practice frameworks, getting the basic principles of security right is a good place to start. Perceived by some as a black art, security hardening checklists can now be delivered in a best-practice template that reflects the specific operating system and network environment. With access to a list of recommendations within a matter of minutes, is there really an excuse for continuing to ignore the essentials of IT security?

However, organisations also need a completely infallible way of detecting the presence of malware if and when it does manage to bypass security defences. The back-stop to traditional defences ideally needs to be a real-time alert triggered by any change to file structure that might indicate compromise or the beginning of the slow move towards the central core of the business.

File Integrity Monitoring (FIM) is proven to radically reduce the risk of security breaches – indeed it is a core recommendation of the PCI DSS and other security standards. It raises an alert related to any change in underlying, core file systems – whether that has been achieved by an inside person or an unwittingly phished employee introducing malware, or some other zero-day threat blasting unrecognised through the AV. Flagging up changes in this way ensures there is no chance of an APT gaining hold, no risk of the stealth attack that gets in and out leaving no trace – there is a trace and the business is immediately notified.

AV and FIM versus the zero-day threat

The key point to note from the previous description of AV operation is that the virus must either be 'known' – ie, the virus has been identified and categorised by the AV vendor – or that the malware must 'exhibit characteristics associated with malware' – ie, it looks, feels and acts like a virus.

Anti-virus technology works on the principle that it has regularly updated 'signature' or 'definition' lists containing details of known malware. Any time a new file is introduced to the computer, the AV system has a look at the file and if it matches anything on its list, the file gets quarantined.

"A FIM system will detect the related unusual file system activity – either at the point at which the malware is introduced or when the malware becomes active"

In other words, if a brand new, never-seen-before virus or trojan is introduced to your computer, it is far from guaranteed that your AV system will do anything to stop it. Ask yourself – if AV technology was perfect, why would anybody still be concerned about malware? Also, why else would the AV need to update every day – or indeed, more frequently – unless it was permanently ignorant of emerging zero-day threats?

The lifecycle of malware can be anything from one day to two years. The malware must first be seen – usually a victim will notice symptoms of the infection and investigate before reporting it to their AV vendor. At that point, the AV vendor will work out how to counteract the malware in the future, and update their AV system definitions or signature files with details of this new malware strain. Finally, the definition update is made available publically – individual servers and workstations around the world will update themselves and will thereafter be rendered immune to this virus. Even if this process takes a day to conclude then that is a pretty good turnaround – after just one day the world is safe from the threat.

However, up until this time the malware is a problem. Hence the term 'zero-day threat' – the dangerous time is between 'day zero' and whichever day the inoculating definition update is provided.

By contrast, a FIM system will detect the related unusual file system activity – either at the point at which the malware is introduced or when the malware becomes active, creating files or changing server settings to allow it to report back the stolen data.

Where is FIM better than AV?

As outlined previously, FIM needs no signatures or definitions to try and second guess whether a file is malware and it is therefore less fallible than AV. Where FIM also provides distinct advantages over and above AV is that it offers far better preventative measures than AV. Anti-virus systems are based on a reactive model, a 'try and stop the threat once the malware has hit the server' approach to defence.

An enterprise FIM system will not only keep watch over the core system and program files of the server, watching for malware introductions, but will also audit all the server's built-in defence mechanisms. The process of hardening a server is still the number one means of providing a secure computing environment, and prevention – as we all know – is better than cure. Why try and hope your AV software will identify and quarantine threats when you can render your server fundamentally secure via a hardened configuration?

Add to this that enterprise FIM can be used to harden and protect all components of your IT estate – including Windows, Linux, Solaris, Oracle, SQL Server, firewalls, routers, workstations, POS systems, etc – and you are now looking at an absolutely essential IT security defence system.

Gold standard

Yet, to date, too many organisations have failed to implement FIM for fear of the additional work load created by a system that flags every single unauthorised change – a fact that says rather too much about the anarchic attitudes towards change management endemic within most organisations. FIM raises an alert for every unauthorised change

that occurs within the infrastructure. For organisations with robust change management processes, with clearly defined patch windows and no changes made without request and authorisation, implementing and running FIM is a breeze: the only time alerts are flagged are when actual security concerns arise.

So how can organisations implement effective change management processes? There are four main types of changes within any IT infrastructure:

- **Good planned changes** – expected and intentional, which improve service delivery performance and/or enhance security.
- **Bad planned changes** – intentional, expected, but poorly or incorrectly implemented, which degrade service delivery performance and/or reduce security.
- **Good unplanned changes** – unexpected and undocumented, usually emergency changes that fix problems and/or enhance security.
- **Bad unplanned changes** – unexpected, undocumented, and which unintentionally create new problems and/or reduce security.

A malware infection, intentionally by an insider or external hacker, also falls into the last category of bad unplanned changes. The same goes for a rogue developer implanting a backdoor into a corporate application. The fear of a malware infection, be it a virus, trojan or an APT, is typically the main concern of the CISO and it helps sell security products – but should it be so?

A bad unplanned change that unintentionally renders the organisation more prone to attack is a far more likely occurrence than a malware infection, since every change that is made within the infrastructure has the potential to reduce protection. Developing and implementing a hardened build standard takes time and effort, but undoing painstaking configuration work only takes one clumsy engineer to take a shortcut or enter a typo. Every time a bad unplanned change goes undetected, the once secure infrastructure becomes more vulnerable to attack so that when your organisation is hit by a cyber-attack, the damage is going to be much, much worse.

Closed loop and total change visibility

The first step therefore is to get a change management process – for a small organisation, just a spreadsheet or a procedure to email everyone concerned to let them know a change is going to be made, at least gives some visibility and some traceability if problems subsequently arise. Cause and effect generally applies where changes are made – whatever changed last is usually the cause of the latest problem experienced.

This is why, once changes are implemented, there should be some checks made that everything was implemented correctly and that the desired improvements have been achieved (which is what makes the difference between a good planned change and a bad planned change).

"What you can't see, you can't measure and, by definition, unplanned changes are typically performed without any documentation, planning or awareness"

For simple changes – say a new DLL is deployed to a system – this is easy to describe and straightforward to review and check. For more complicated changes, the verification process is similarly much more complex.

Unplanned changes, good and bad, present a far more difficult challenge. What you can't see, you can't measure and, by definition, unplanned changes are typically performed without any documentation, planning or awareness.

Contemporary change management systems utilise FIM, providing a zero tolerance to changes. If a change is made – configuration attribute or to the file system – then the changes will be recorded.

In advanced FIM systems, the concept of a time window or change template can be pre-defined in advance of a change to provide a means of automatically aligning the details of the RFC (Request for Change) with the actual changes detected. This provides an easy means to observe all changes made during a planned change, and greatly improve the speed and ease of the verification process.

FIM and configuration hardening

Which brings us to the subject of configuration hardening. Hardening a configuration is intended to counteract the wide range of potential threats to a host and there are best practice guides available for all versions of Solaris, Ubuntu, RedHat, Windows and most network devices. Known security vulnerabilities are mitigated by employing a fundamentally secure configuration set-up for the host.

For example, a key basic for securing a host is via a strong password policy. For a Solaris, Ubuntu or other Linux host, this is implemented by editing the /etc/login.defs file or similar, whereas Windows hosts will require the necessary settings to be defined within the Local or Group Security Policy. In either case, the configuration settings exist as a file that can be analysed and the integrity verified for consistency (even if, in the Windows case, this file may be a registry value or the output of a command line program).

Therefore file integrity monitoring ensures a server or network device remains secure in two key dimensions: protected from trojans or other system file changes, and maintained in a securely defended or hardened state.

Is it the right file to begin with?

However, is it enough to just use FIM to ensure system and configuration files remain unchanged? While there is a guarantee that the system being monitored remains in its original state, keep in mind that there is a risk of perpetuating a bad configuration, a classic case of 'junk in, junk out' computing. In other words, if the system is built using an impure source, then the system will be maintained in its original, but bad, state. The recent Citadel keylogger scam is estimated to have netted over $500m in funds stolen from bank accounts where PCs were set-up using pirated Windows DVDs, each one with keylogger malware included free of charge.

In the corporate world, OS images, patches and updates are typically downloaded directly from the manufacturer website, therefore providing a reliable and original source. However, the configuration settings required to fully harden the host will always need to be applied and in this instance, file integrity monitoring technology can provide a further and invaluable function.

"All hosts can be guaranteed to be secure and set-up in line with not just industry best practice recommendations for secure operation, but with any individual corporate hardened build standard"

The best enterprise FIM solutions will therefore not only detect changes to configuration files/settings, but also analyse the settings to ensure that best practice in security configuration has been applied. In this way, all hosts can be guaranteed to be secure and set-up in line with not just industry best practice recommendations for secure operation, but with any individual corporate hardened build standard. It is for precisely this reason that a hardened build-standard is a pre-requisite for secure operations and is mandated by all formal security standards such as PCI DSS, SOX, HIPAA, and ISO27K.

Conclusion

The temptation to rely on AV is understandable: in an overworked IT department any set-up-and-go system has appeal. But in an era that is increasingly dominated by the APT, relying on AV is not just complacent it is ill-judged. Organisations need to safeguard data – from customer records to intellectual property – against organisations with phenomenal reach and expertise, as well as a willingness to play the waiting game.

Good data protection requires all available security technologies to be deployed in harmony to give you a fighting chance of defending your organisation's digital assets. But there will never be any substitute for sound adherence to best practice security measures. Good change control and device hardening – for example, no default user accounts, always named user accounts being used, restricted assignment of privileges to users – the list goes on, but with technology used to automate the checks and balances required to operate best practice measures.

The risks have changed. The threat is stealthy and targeted. It is time not just to pick the right battle – but to arm the business with the right defences.

About the author

Mark Kedgley is chief technical officer at New Net Technologies where he is responsible for driving ongoing product development; his primary objective being to continually push New Net Technologies' data security and compliance solutions to protect their customers' sensitive data against security threats and network breaches.

References

1. 'Improving Critical Infrastructure Cybersecurity'. NIST. Accessed Jan 2014. www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

The quest for clarity on data protection and security


Peter Heim

Peter Heim, Dell SecureWorks

The European data protection laws have some of the highest standards in the world. As the laws continue to evolve, there is a lot of ambiguity from one country to the next about what that means for businesses. The reality is that there is little clarity to help fully understand the European data protection law and how it directly or indirectly applies to every organisation that handles data. For that reason, legal awareness is paramount for businesses to make efficient use of their resources, thereby enabling them to achieve better data security and meet the requirements of the law.

Skills and resources

With the growing array of security threats, a high priority for businesses must be ensuring they can protect themselves in order to trade effectively. Many organisations have understood that information security is becoming increasingly specialist but they do not have the skills or resources to effectively build, manage and monitor a secure environment or understand the latest threats and trends. This leaves many organisations at risk of breaches, downtime and non-compliance.

Although there are certain measures businesses can proactively take to protect their intellectual property, often a more effective and efficient approach is to work with a trusted third party, such as a Managed Security Service Provider (MSSP), to provide expert help in managing security infrastructure and monitoring for threats 24/7. This lowers cost, increases security posture and allows internal staff to focus on key initiatives.

Despite the benefits of using a MSSP for an organisation's security posture, a number of common misconceptions