Defending against the malware flood


Greg Sim

Greg Sim, Glasswall Solutions

The deluge of new malware specimens being launched against businesses everywhere on the planet is fast rendering traditional anti-virus (AV) cyber-security redundant.

Analysts at German anti-virus vendor G Data have calculated that the birthrate of malware has now increased from one every 4.6 seconds in 2016 to one every 4.2 seconds in the first quarter of this year. The company estimates that 6.834 million new malware specimens were created in 2016 and that 1.853 million were launched into cyberspace in the first quarter of last year – an increase of nearly 73%.

It certainly begs the question as to how signature-based cyber-security can function when new malware is being produced on such an industrial scale every second. Yet it is not a question that appears to trouble enough people responsible for protecting businesses. Even though this flood of new variants is evidence that we are entering a new era of malware invention, organisations still rely on old AV defences that require the identification of malware signatures before they can work out what to block.

It is not surprising then, that Ian Levy, the technical director of the UK's National Cyber Security Centre (NCSC), recently felt it necessary to warn that cyber defence technologies from traditional suppliers will be unlikely to protect organisations in five years' time.

Bespoke files

What makes this situation so much worse is the remarkable cunning of the criminals producing the malware, who know how to circumvent conventional AV-based perimeter security. Instead of wasting their time sending out one file to thousands of recipients like traditional email scammers, criminals are wrapping up their malware in a new email file for each recipient, which makes each exploit extremely difficult for conventional perimeter defences to identify and block.

Criminals are fully aware of this. AV technology has to conduct a complete inspection of each file and drop anything suspicious into the process to achieve validation before it writes a signature. The signature must then be pushed out to update every endpoint. This leaves organisations using AV security unprotected and exposed for a dangerous amount of time.

The right direction

In response to these new threats, some organisations have started using technologies such as Content Disarm and Reconstruction (CDR) to protect themselves. Although this is a step in the right direction, it will not provide a bullet-proof defence against the most common form of attack – the malicious code secreted in an innocent-looking email attachment. Solutions sold under the CDR heading will extract suspicious items or content from a file, but tests have shown they will not pick up the minute alterations to a file and its structure that can be used to trigger malware downloads.

In order to bar all malware hidden in email attachments – such as PDFs or Word files – file-regeneration technology is necessary. This inspects each document down to byte level against the manufacturer's standard, eliminating everything that should not be there. Instead of hunting for known viruses, it produces a clean, sanitised and safe version of a document within fractions of a second.

The requirement for file regeneration grows every day as new malware variants proliferate which are shaped according to their target. Analysis among a broad cross-section of organisations using file-regeneration technology shows that three-quarters of the malware it is disarming is unique to the organisation being targeted. In a 30-day period alone, 37 viruses were stopped that were unknown to either clients or Virus Total, which amounted to 73% of the total blocked. More depressingly, over several months this year, file-regeneration technology found that out of 5,575 separate malware types it prevented from entering organisations, 99% already had signatures and should have been picked up by the AV defences that were in place at the perimeter. In some cases, almost 600 pieces of unstoppable malware of one form or another were prevented from reaching individual organisations in a single day.

This is in line with research from respected cloud services and threat intelligence company Webroot, which earlier this year confirmed the trend for criminals to use discrete files, demonstrating that 97% of malware is now unique to a specific endpoint.

Email security

We know that the vast majority of successful cyber-attacks are delivered via everyday email attachments. Verizon's authoritative research found that 66% of malware was installed via malicious email attachments.

Criminals hide their zero-day attack triggers inside the content or, as is more often the case, in the structures of common file-types. Malware can come into organisations as extensible features such as macros, AcroForms, embedded files, hyperlinks and in JavaScript. However, analysis shows that it is the structures of common files that criminals now most commonly use to hide malicious exploits.

Unfortunately it only takes a single click from an unwitting employee for malware to be downloaded and the organisation compromised. The sophistication of social engineering makes it extremely difficult for hard-pressed employees at any organisation to avoid clicking on a link or opening an attachment that appears to be an invoice or purchasing order from a known business or supply chain partner.

Research among 2,000 office workers in the US and UK this year reveals how staff feel they are not being given the right tools to help them protect the organisations they work for, and how they also have inadequate understanding of the risks of clicking open a phoney email attachment. The majority (62%) of those surveyed admitted they do not usually check the legitimacy of email attachments that come from unknown sources.

Inventive criminals

Cybercrime is now a hotbed of industrial creativity and the push to produce new malware variants is unlikely to cease in the foreseeable future. Locky ransomware variants, for example, are proliferating and threaten increasing numbers of businesses, turning up in a 'double-zip' form. This is often accompanied by the Kovter Trojan, which is left behind to run click-fraud and malvertising even after organisations have paid up. Locky is also being adapted to exploit old vulnerabilities in Microsoft's Dynamic Data Exchange (DDE), a feature that allows the transfer of data between Windows applications.

Yet although businesses are finally waking up to the realisation that the big players in anti-virus technology can no longer protect them, many organisations seem to regard extortion via cyber-attack as an inevitable cost of business or mistakenly believe they can, if necessary, fall back on their insurance.

Investment in innovation

This is a very misguided stance. Accenture and the Ponemon Institute recently reported that the cost of cyber breaches has reached $11.7m per organisation and every day brings more news of successful cyber-attacks that threaten to plunge a business into devastating losses. The advent of the European Union General Data Protection Regulation (GDPR) and its potential for hefty fines, public disclosure and even jail sentences in the event of serious data breaches should focus minds very sharply. Of course, security is not all about technology. Staff awareness will lift an organisation's security posture too, but it can only go so far.

Given the failing nature of AV security and the ability of file-regeneration technology to counter all exploits, irrespective of whether they have been assigned signatures, it is time for organisations to overcome their natural conservatism and invest in innovation. File regeneration, which looks only for the known good in each file, keeps every form of malware at the door and puts security policy back in the hands of businesses. A business can decide, for example, which department needs access to macros and determine what are acceptable levels of risk across the organisation.

Faced with highly inventive criminals who are creating such huge volumes of new malware, organisations must innovate if they are to protect themselves. It is a question of only allowing the known good to enter an organisation and being fully confident that the main source of zero-day threats has been completely blocked.

This is far more effective than relying on porous old perimeter anti-virus security that can never keep up with the millions of new malware types produced every year.

About the author

Greg Sim is the CEO of Glasswall Solutions, who, as a founding director, was instrumental in building the current team and establishing its intellectual property and patents. He is a cyber-security veteran of over 10 years.

The intelligent way to protect complex environments

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Technology is becoming ever more complex, IT environments increasingly labyrinthine and the threat landscape is expanding, seemingly exponentially. This is mirrored in the sophistication – but also complexity – of defensive systems. Information security specialists now face a deluge of information and deciding what is significant isn't easy. In this interview, Ed Bellis, CTO of Kenna Security, talks about the challenges facing organisations today and how an intelligent approach to security data can help organisations spot the genuine threats.

Kenna says he understands the frustrations of CISOs because he used to be one.

"One of the things that was continuously difficult for us on the security team," he says, "was being able to deal