The fight against cyber crime requires innovative defence

By Sam Hutton, CTO at Glasswall Solutions

Cyber crime has been making a rapid ascent in the list of priorities for many organisations as they see the catastrophic damage – both financial and reputational – it has wreaked on enterprises across the world. In looking for the best defence, many of these organisations have come to the conclusion that a new and innovative solution is needed.

As cyber attacks continue to become more common and even more impactful on the organisations who fall victim to them, they are also becoming more prevalent on the world stage. At the latest World Economic Forum, for example, cyber security was made a main point of discussion. While some attendees called it the largest challenge currently facing organisations, others said the fear of falling to a data breach was responsible for companies becoming increasingly cautious of adopting new technologies.

The growing awareness of cyber attacks isn't limited to business, however, as governments across the globe place more focus than ever on cyber security awareness. In the UK, for example, the Chancellor of the Exchequer released a five-step plan last year to increase cyber security.

In the US, meanwhile, the proposed Cybersecurity Disclosure Act would require public companies to give reasons for not having a cyber security expert on the board. In the EU, after the European General Data Protection Act comes into effect in 2018, organisations will risk stiff fines if they suffer data breaches or are found to be negligent around security.

Not surprising then that CISOs in enterprises industry wide are under pressure to be innovative and to find new, but cost-effective, solutions. They are fully aware that they will be held accountable in the event of a serious data or security breach.

If the new focus on cyber security is to work, however, all involved need to realise that constantly-evolving threats require constant innovation, rather than just post-infection BAND-AID. Criminals have moved on from what are commonly called signature-based threats, to instead placing increased attention to altering the structure of common file-types to defeat existing security and anti-virus solutions and breach an organisation's defences.

As the evolution and sophistication of these threats becomes clear, it is time for all organisations to grasp that cyber criminals are not gifted amateurs, but sophisticated professionals determined to

steal funds or shadowy arms-length state organisations with significant resources dedicated to the theft of intellectual property. Between them they never stop experimenting and evolving.

When faced with such ingenuity, legitimate businesses cannot afford to fall behind in the race to innovate and need to reassess their level of skill and motivation.

Most fundamental of all, CISOs have to understand that traditional signature-based AV security no longer cuts the mustard. Email attachments are still the most common delivery mechanism for the malicious code that enables criminals to steal, destroy or hold data to ransom, but how they are used has changed.

Analysis of many thousands of files by Glasswall shows that while extensible features such macros and embedded files remain significant dangers, criminals are now well-advanced in altering the underlying structure, or building blocks, of Word, Excel, PowerPoint files and PDF files, so that once opened they will trigger a malicious exploit. In PDFs, for example, Glasswall has found that structural threats are close to outweighing those hidden in embedded files, AcroForms, Javascript or some combination of these elements.

The only effective solution to defend against this deliberate corruption of email-bound documents lies in file-regeneration technology. An automated solution utilising this capability disarms malicious files, producing a benign version referenced against the manufacturer's original standard, checking it right down to byte level instead of just looking for active content in the body of the document. A sanitised file is regenerated at sub-second speeds and passed on to users in real-time to maintain business continuity.

The technology protects organisations against even the smallest and most subtle alterations in file structure, detecting for example, where criminals have changed just two bytes in a PDF file to crash the reader software in order to trigger malware or hidden exploits.

This is a solution devised after long and pioneering experience in the "Content Disarm and Reconstruction" (CDR) sector. After all, obtaining a completely benign file is a hugely complex process which, for a PDF, requires 3,500 conformity checks in much less than a second.

Rival technologies based on transformation alone rather than regeneration are simply less effective at removing threats, often producing un-editable PDFs or JPEGs which significantly disrupt business continuity.

Transformation technologies also frequently make the same mistake as those they seek to supplant, searching for what is already known, since they are often incapable of removing new threats that

have no name or signature. For example, AcroForms are known to carry malware and are one of the focus areas for CDR technology. However, Glasswall analysis has shown AcroForm threats can be removed from a PDF while leaving 80 per cent of malicious content intact.

Besides blocking out known and evolving threats, one of the great benefits of file-regeneration is that it puts organisations back in control, deciding who should receive specific file content as part of a broader security posture. It means individual employees no longer have to make decisions about whether it is safe to open files.

The overall outcome is that organisations can send and receive emailed documents from customers, partners and suppliers in full confidence and which in turn are safer to do business with. It is clear that only the kind of genuine innovation to be found in file-regeneration solutions will give organisations this watertight level of security and streamlined efficiency. In the face of so many emerging threats it is vital that the CISO recognises this important fact in the ongoing battle against cyber crime.

-Ends-