Glasswall whitepaper

Prevention Is Better Than Cure

Shining the light on rapidly changing cyber threats

GLASSWALL

CONTENTS

INTRODUCTION

The scale of cybercrime and the threat from malware is now widely understood right across the international business community.

However, along with this growth in awareness comes a dangerous degree of complacency.

Major data breaches such as those at TalkTalk, Target and Experian have led to public humiliation and serious commercial damage and are the consequences of failed approaches to cyber security which rely on signature-based detection, out-dated technologies and mindsets.

As a result of its data breach in October 2015, for example, telecoms giant Talk Talk lost more than 100,000 customers and suffered £60 million in costs and disruption. The Experian hack put the personal details of 15 million customers at risk and badly tarnished the organisation's reputation as a global information-services and credit monitoring company.

All round the world, the email attachment is known as the most common delivery vector for the malicious code used by criminals and commercial rivals to steal information, hold an organisation to ransom or inflict widespread disruption.

To reinforce the point, Cisco last year alerted the cyber world to a 50 per cent increase in email attacks employing macros as the cause of infection. Locky ransomware, for example, emerged earlier this year (2016) infecting 400,000 computers in a few hours and has continued to aquire up to five more machines every second. It was delivered in a Microsoft Word attachment containing macros.

In the face of these growing threats, Glasswall has undertaken innovative research that for the first time highlights some unique insights into what weaponised files look like and turns conventional thinking about cyber security on its head.

NEW THREATS REQUIRE NEW TECHNOLOGY

Using the unique capabilities of Glasswall's regeneration engine, deep analysis of thousands of files demonstrates that the biggest threat to the cyber integrity of businesses now comes from within the structure, or building blocks, of common file types such as PDFs, Word, PowerPoint and Excel.

This is a fast-emerging trend which many organisations have not yet fully grasped. The majority are deploying security solutions that search in the wrong places and are designed to detect and remove previously identified threats or signatures, when the reality is that criminals have moved on.

Research (from respected cloud services and threat intelligence company Webroot) has for example demonstrated that 97 per cent of malware is now unique to a specific endpoint. This renders signature-based security virtually useless because such heavily customised malware is extremely difficult to detect.

The new forms of malware are in a constant state of development, operating outside the scope of conventional signature-based or AV security in which the majority of businesses place their trust.

While organisations understand the threats within JavaScript, Flash, encrypted and embedded files, they are in fact overlooking the biggest sources of danger which are actually inside the structures of common files.

Unfortunately the belief that macros (pieces of code that may have legitimate use within a document) are the chief menace to security is widespread. Microsoft, for example, says 98 per cent of threats targeting Microsoft Office use macros.

1. Unknown or Malicious Documents

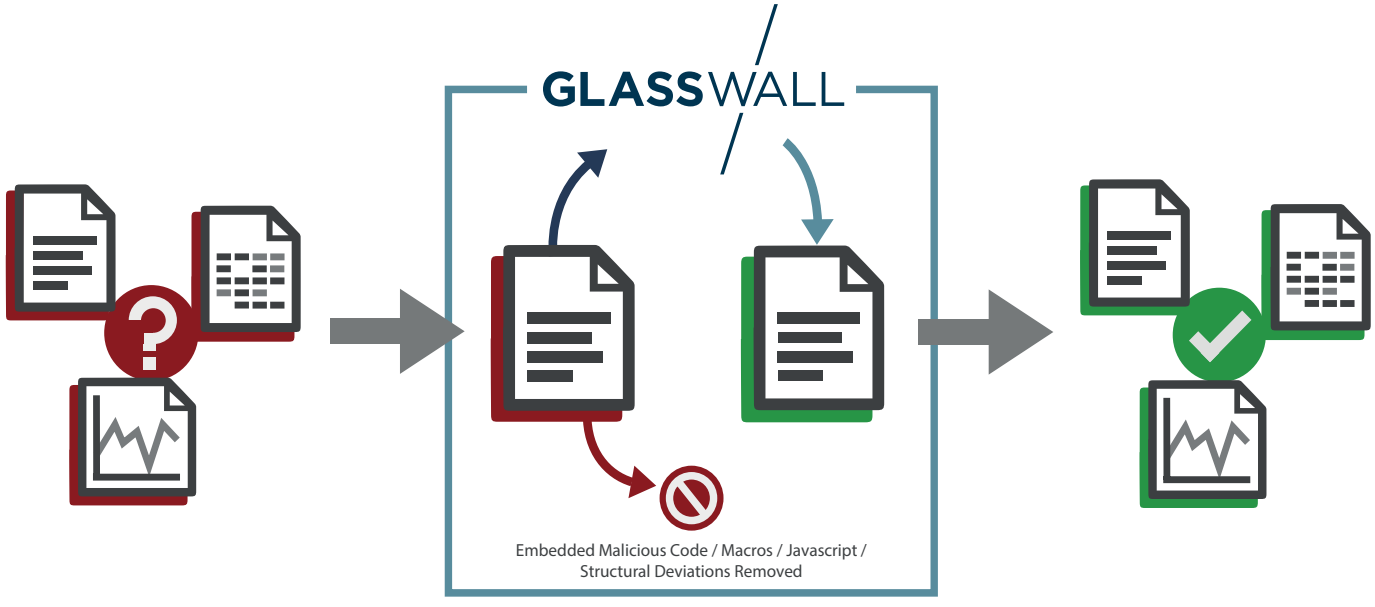
- Unknown
- Non-compliant
- Structural & functional risk
- Potentially malicious

2. Files Inspected and Regenerated

- Analyses and reports on files
- Applies policy to embedded and extensible items
- Signatureless, no updates

3. Only Clean, Usable and Benign Files Pass

- Disarmed scripts / macros / embedded threats
- Fully standardised files
- Original content untouched
- Real-time delivery



THE INADEQUACY OF CONVENTIONAL SECURITY

Reliant on incomplete and out-dated intelligence about the nature of the threats they face, businesses continue to place their trust in traditional anti-virus defences who require the identification of a threat before it can be detected. In other words, someone has to become its victim before the industry is aware of it and gives it a signature.

This year's massive Cerber ransomware attack, for instance, which targeted Microsoft Office 365 users, proceeded for 24 hours before it was detected and the industry started putting blocking measures in place.

Since signatures have to be established and circulated for anti-virus defences to be effective, this inevitably leads to a constant time-lag before security against a particular piece of malware is assured. The result of this delay is that conventional anti-virus defences are often little more than 45 per cent effective.

Vendors also claim that a 19 per cent increase in the detection of malware can be achieved through the addition of a second anti-virus solution. While this may sound significant, it is in fact only 19 per cent of the original 45 per cent security attained by a primary AV solution, indicative of a law of diminishing returns that will never ensure complete protection.

While macros and embedded files remain dangers, Glasswall's unique research now reveals that criminals are in fact devoting their considerable resources and talents into altering the underlying structures of the files themselves.

ANALYSIS SHOWS THE SCALE OF THE THREAT WITHIN FILES

To assess the scale and nature of the evolving threat landscape, Glasswall has analysed tens of thousands of PDF, Word, PowerPoint and Excel files. The research is unique because, unlike competitors who try to identify viruses and malware, Glasswall is quantifying the anatomy of attacks. The results now make plain that conventional AV security approaches will not deliver complete protection.

THE RESEARCH SHOWS THAT:

- In PDFs, the trend is now at tipping point for structural threats to outweigh those hidden in embedded files, AcroForms, JavaScript or in some combination of these elements.
- Over a three month period, between 70 and 90 per cent of issues were found within the structure of the PDFs, compared with no more than 20 per cent for threats inside AcroForms, JavaScript, embedded files, or some combination of these elements.
- Malware is more likely to come in the form of an embedded file in PowerPoint than in Word or Excel.
- Macros are much more likely in Word and Excel files and less prominent in PowerPoint.
- Within a single week, organisations relying on the identification of macros can miss 45 per cent of other malware in Word documents.
- Trends fluctuate from week to week, but across all document types, structural threats are fast-growing.

The message coming loud and clear from this continuing research is that the nature of the threat landscape is constantly shifting and that organisations cannot simply rely on tracking and stopping known malware. Focusing on known bad exploits as the source of danger leaves an organisation open to successful attacks from the criminals' rocketing use of adaptations to the structures of files.

Sophisticated and organised, criminals are now capable of manipulating vulnerabilities within the complex file structures so that as soon as they are opened, malicious code will automatically contact a remote server and download malware.

This is malware that may hold an organisation to ransom or gather intelligence within a system for months, siphoning off intellectual property, highly sensitive customer details or simply logging the employees' key strokes to give access to accounts and data vaults.

While the common belief is that malware will reside on a system for an average of 200 days, in truth, nobody knows the true lifespan of these malicious pieces of code that are in constant and secret communication with the machines of the criminals who control them.

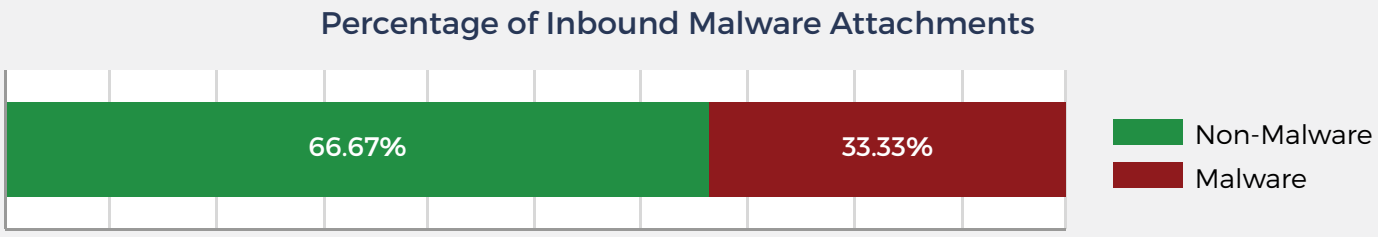
In August this year (2016) the Project Sauron malware was found to have laid undetected in the systems of scientific, military, telecoms and financial organisations for five years, capable of disguising itself as other files and spying extensively on infected computers.

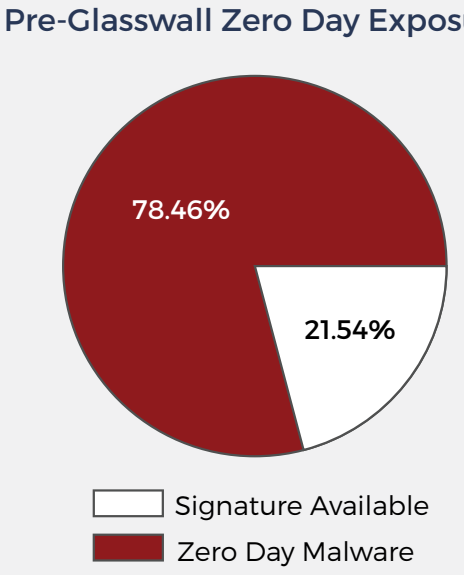
In the face of these threats, the deployment of cyber security solutions that detect known signatures is a deeply misguided and dangerous approach when file regeneration technology can eliminate unidentified threats.

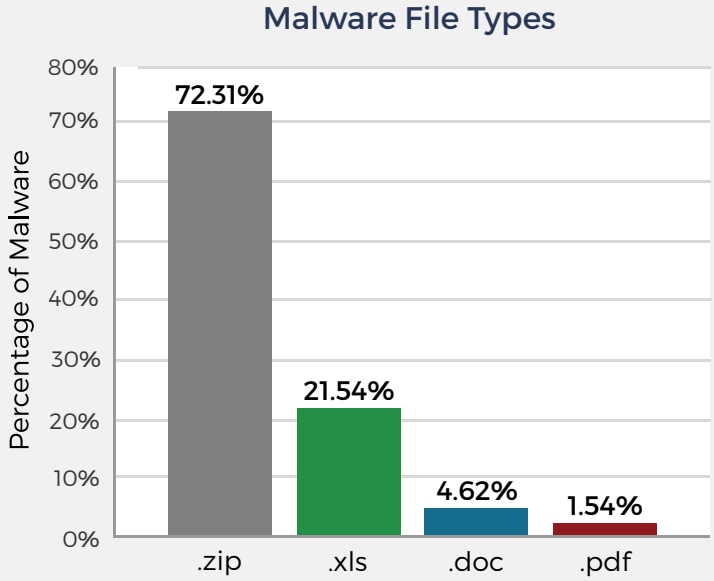
The industry is in danger of sticking with a blinkered focus on detecting breaches after the event, resigning itself to the wholly mistaken belief that threats cannot be stopped at source.

Instead of committing major resources to such cyber security fire-fighting, businesses need to concentrate on solutions that prevent the arsonists gaining any entry to the premises and which are guaranteed to stay one step ahead of sophisticated attackers.

While the industry waits for signatures to be identified and circulated, Glasswall technology can block all threats, known and unknown, in real-time, regenerating sanitised files in sub-second speed so that all anomalies and malicious exploits are left outside the organisation, while at the same time guaranteeing full business continuity.







Threat Intelligence for Glasswall Solutions' email traffic September 2016

REGENERATION TECHNOLOGY IS THE COMPLETE DEFENCE

Glasswall has a highly innovative answer to solving the single biggest threat from these criminals – the deliberate corruption of email-borne documents.

Glasswall's automated solution disarms malicious files, producing a benign version measured against the manufacturer's original standard. Instead of searching for active content within the body of the file, Glasswall examines each file for conformity.

Each attached file is broken down to byte level and checked. It is then regenerated as a sanitised file at sub-second speeds and passed on to users in real-time to maintain business continuity.

The solution can render a file safe against even the smallest and most subtle alterations, 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.

The Glasswall approach works for two reasons. Firstly, because files will no longer conform to the standard if cyber criminals have even minutely tampered with them. Secondly, because as Glasswall research shows, it is in the file's structure that most of the threats to cyber security now lie.

It is important to emphasise here that there is no link between the number of anomalies within a file and the degree of threat. A benign file may, for whatever reason, have as many as five million anomalies, but remain perfectly benign. Fortunately, for users of Glasswall, this is not something they have to worry about.

Indeed, Glasswall has far longer experience of overcoming the severe technological challenges in Gartner's "Content Disarm and Reconstruction" (CDR) sector than any other vendor. Obtaining a completely benign file is a complex process which, for a PDF, requires 3,500 conformity checks in much less than a second.

Rival technologies based on transformation rather than regeneration are less than wholly effective at removing embedded features and extensible objects and are even liable to insert elements of their own. They also often fail to recreate files in an editable format, producing PDFs or JPEGs which do not meet the needs of users and of course, which disrupt business continuity.

A common feature of CDR technologies is that they make the same mistake as those they seek to supplant, searching for what is already known and thereby ignoring the true nature of the threats faced by organisations.

For example, AcroForms are known to carry malware and are one of the focus areas for CDR technology. However, Glasswall analysis shows it is perfectly possible to remove AcroForm threats from a PDF while leaving 80 per cent of malicious content intact.

Glasswall also re-optimises sandbox technology, boosting its role as a source of intelligence about the evolving characteristics of threats, while reducing the time and resources required to make it operational. Additionally, since it is an in situ technology that does not require signature updates, Glasswall is able to reduce management overheads in a company's cyber security operations.

THE IMPORTANCE OF BEING IN CONTROL OF POLICY ON FILES AND DOCUMENTS

Glasswall's unique approach is hugely important in putting organisations back in control, deciding who should receive which file type content as part of a policy of managed risk.

Departments that require files with macros or other features for their everyday working are permitted safe access to them in accordance with guidelines. It means business continuity is never affected.

It may be, for example, that a business decides that only its finance department should receive Excel spreadsheets and macros, whereas its supply chain partners will be barred from sending PDFs.

The goal of automation in this context is for any user to open a file and be confident he or she will not infect the company. While employees carry on with business as usual, the technology is constantly working to protect the business in the background. Policy decisions of this kind can be logically updated using actionable risk intelligence, enabling effectiveness to be measured through continual analysis.

The overall outcome is that organisations can send and receive emailed documents from customers, partners and suppliers in full confidence. Glasswall has spent over eight years in research and development on its solution, fine-tuning the perfect solution that allows businesses to become trusted by all their partners and customers and gain a significant edge over the competition.

CONCLUSION

In a world of highly-professionalised cyber crime, the continued reliance on signature detection is leaving businesses extremely vulnerable to threats hidden in places they are failing to search.

Reliance on finding known bad signatures is futile when the methods used by criminals are in a permanent state of evolution and therefore cannot be detected. In fact, so many millions of signatures are being created it is impossible now to use them as an effective end-point security tool.

Glasswall by contrast, has in the course of file analysis and regeneration, discovered malware that only a quarter of conventional anti-virus vendors had picked up and were capable of preventing three days later. In many instances >75% of the industry have created a signature for a piece of malware Glasswall stopped a week earlier.

The consequences of pursuing this approach are potentially dire. Once organisations have been breached or blackmailed, cyber and risk teams will be held responsible and chief executives will have to make detailed explanations to customers and shareholders.

Instead, through Glasswall, the technology is available to sanitise every file, regardless of what new exploit the criminals may devise, ensuring that no malicious element penetrates the organisation.

SMEs are also dangerously exposed, often lacking the financial resources to adequately protect themselves. More than 80 per cent of SMEs erroneously believe themselves too small to be targeted, even though by far the vast majority of hacking attacks are perpetrated against them.

Many still rely on perimeter AV security, which makes them a highly visible and attractive route into the systems of enterprise-level clients and their entire supply chains.

Whatever the size of an organisation's cyber security budget, money alone will not guarantee protection. All organisations must accept the basic truth that prevention is better than cure as criminals constantly develop new exploits.

As research by Glasswall demonstrates, the single biggest threat to all businesses continues to be the email attachments that are now indispensable to day-to-day operations.

The research shows a strong and increasing trend towards the manipulation of the structures of documents, rendering conventional signature and active content-based security ineffectual. Any organisation concentrating on macros or embedded files is failing to prevent the majority of the threats it now faces, opening its vaults to criminals and leaving it vulnerable.

While vendors with technologies in the CDR sector may claim their solutions will reconstruct versions of files that are clean of malware and free from threats, in reality they too are blinkered, searching in the wrong places.

Many of these companies employ a snapshot approach and employ what are in effect, sub-features of Glasswall technology. The result is the same dangerous neglect, which leaves organisations vulnerable to malicious code written into the structure of some of the most common file-types in business.

It is time for everyone in business and cyber security to completely rethink their outlook and admit that the era of traditional AV solutions, signature and active-content based security, has passed.

Criminals are more cunning than ever and these approaches will never keep up with their ingenuity. Instead, through Glasswall, the technology is available to sanitise every file, ensuring that no malicious element penetrates the organisation to do it damage.

Organisations become secure, confident and far more efficient as they devote less resources to protecting themselves from cyber threats. Trusted by customers and partners, they are back in control, using the technology's in-built flexibility to ensure business operations are fully optimised and impregnable to compromise.

GLASSWALL

CONTACT US FOR A FREE TRIAL

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652

info@glasswallsolutions.com
www.glasswallsolutions.com