Dr Simon Wiseman, CTO of Deep Secure

TRANSFORMING CYBERSECURITY

The Bank of England and the Financial Conduct Authority have informed the financial services sector that they must meet new standards in operational resilience and cybersecurity in the face of a state of near constant cyberattack.

Reflecting on the 'attack surface' of the typical financial sector organisation, Dr Simon Wiseman, CTO with UK Cybersecurity firm Deep Secure, looks at the potentially vulnerable areas and suggests ways to mitigate the risks.

Guarding the Gateway

Many of the cybersecurity attacks initiated against organisations in the financial services sector start with an exploit or threat concealed in seemingly innocent business content arriving into the corporate network via the email or Web gateway. Whatever the vector and whatever the precise nature of the threat, time and again it is business content – documents, spreadsheets, presentations and images - that are used to conceal the attacker's intent.

Traditionally, the job of combatting threats concealed in business content arriving at the email and Web gateways have been given to detection-based cybersecurity defences, as typified by anti-virus and anti-malware products. The problem now is that these defences are proving wholly inadequate in the face of increasingly sophisticated cybercriminals. Attackers are now employing against commercial targets the kind of sophisticated zero-day, stealthy exploits that were hitherto the province of nation-state intelligence entities.

Fortunately, new ways of combatting this type of threat are emerging, and one of the most effective is called Content Threat Removal. Content Threat Removal doesn't attempt to detect the presence of a threat in business content arriving at the gateway. Instead, it assumes that all content is potentially bad. Using a process called content transformation, it intercepts every document and image, extracts only the valid business information from it, discards the original and creates a brand new, threat-free copy to deliver to the intended recipient. The content transformation process can't be circumvented or evaded because it is not interested in trying to detect anything untoward that the bad guy has hidden in the content. It simply eliminates the risk, even when new forms of attack are devised.

Portal Problems

We're in the age of the self-service portal. Prospects and customers alike are encouraged to upload documents (often in the Adobe Portable Document Format or PDF) in support of everything from personal loans and mortgages to motor insurance applications. The problem is that while the PDF is a versatile and incredibly useful file format, it is also highly complex, easy to subvert and is regularly used by cybercriminals to carry malicious payloads.

A typical response to the threat posed by PDFs uploaded from the Internet or other untrusted sources has been to try and mitigate the risk by scanning them with multiple detection-based anti-virus scanners. The problem as we've already noted is that detection-based defences like anti-virus routinely fail to pick up the latest threats and zero-day exploits. Here again, the best way to mitigate this risk is to re-evaluate the security and deploy a technology that doesn't rely on detection but uses content transformation at the portal boundary to ensure that only PDFs that are completely threat-free are delivered into the network.

The demand for customers to interact with financial service providers by uploading documents via portals is only going to increase, and so is the danger of compromise from malware concealed within those documents. Mitigating this risk to an acceptable level necessitates a rethink of the defences and a willingness to move away from a dependence on detection and towards complete elimination.

Combatting the Undetectable Exploit

When is an exploit undetectable? Well, one answer is when there is no evidence of how the valuables were taken - only the certainty that they've gone! For all the millions spent on highly sophisticated cybersecurity products, the fact is that undetectable exploits keep on occurring. Although there is little certainty over how this is being achieved, what evidence has been uncovered points to the use of exploits that conceal information in images using a technique called steganography.

Image steganography is the attacker's dream tool. It can be used to infiltrate malware, exfiltrate large amounts of value and maintain secret command and control (CnC) channels, all concealed in seemingly innocuous images. Images, of course, are everywhere, and from a simple tweet to the corporate logo in an email signature, each one can be subverted using image steganography. No data loss protection tool can detect whether an image is harmless or dangerous because image steganography is undetectable.

> **"The demand for customers to interact with financial service providers by uploading documents via portals is only going to increase, and so is the danger of compromise from malware concealed within those documents."**

In the face of the threat posed by image steganography, organisations can either decide to ignore the risk (many still do) or address it using a transformative approach whereby every image is intercepted at the boundary and re-created anew before being passed to the intended recipient. This approach doesn't try to detect the exploit; it assumes every image could be compromised and renders them all safe, preventing hidden malware getting in, stopping covert information leaks and blocking stealthy command and control channels.

A Stronger Screen for SWIFT

Thefts via SWIFT have been under the spotlight. SWIFT, the global provider of secure financial messaging services, is the mechanism by which financial organisations exchange financial messages relating to payments, securities, treasury and trade. Since at least 2013, those that use SWIFT within financial organisations have been targets of concerted attack with many banks across world falling victim and incurring sometimes heavy losses. Many of these exploits have involved gaining access to credentials or exploiting vulnerabilities in ageing network equipment. Addressing these issues is obviously good practice, but there are further steps the organisation can take to build a stronger screen for SWIFT users.

There is some evidence that attempts to target SWIFT users may take the form of so-called 'sideways attacks'. To elaborate, the initial penetration takes place via email or Web at the boundary into the corporate network. With a beachhead established the criminals can orchestrate a multi-part attack, whereby malware is triggered on the corporate network to distract the security team while the real target, users with access to SWIFT, is hit 'sideways' from already compromised workstations internally on the network.

As stated earlier, best practice in combatting this type of activity has to be reviewing the boundary defence (email and Web) and deploying cybersecurity technologies that don't rely on detection to identify malware carried in documents but instead transform the content. While not the only answer to a stronger screen for SWIFT adopting this approach will ensure that the incoming business content is rendered 100% threat free.

Building a Crypto Currency Fortress

It's really something of a mistake to think that cryptocurrency security is all down to the cryptography. The real security risk you have to consider is how to keep the coins safe when they are in storage. So you have to think about where the coins are held in the same way as you need to think about where conventional cash is kept.

Ultimately, keeping cryptocurrency coins in a properly designed hardware 'wallet' that is not connected to the Internet, ensures you have full control over them, but it's a manual process and not scalable. Allowing the coins to be controlled by a connected system, means that system has to able to repel all current and future cyberattacks. This kind of 'failure is unthinkable' protection has previously only been associated with defence and intelligence systems but is becoming increasingly important to online cryptocurrency systems. The providers of these systems are going to have to deploy the latest security mechanisms, guarding the system that hosts the keys to ensure they are not compromised, and trust in the entire eco-system is not undermined.

Organisations in the financial services sector are rightly concerned about the attack surface they present to the attacker. Going forward, they must be prepared to reduce their reliance on detection based cybersecurity defences and adopt new technologies such as content transformation if they are to improve their overall security posture.