STEGANOGRAPHY – AN UNCOMFORTABLE TRUTH

Steganography is becoming the concealment technique of choice for the canny cyber criminal. It's available as a standard feature in many of the exploit kits available on the Dark Web and its use is growing. Deep Secure CTO Dr Simon Wiseman looks at why and how it is being used, and asks whether anyone can offer a credible defence against this highly evasive technique.

Hiding in plain sight

Steganography (from the Greek steganos, or 'covered', and Latin graphia, or 'writing') is the hiding of a secret message within an ordinary looking message or file and the extraction of it at its destination.

Sound dull? Well consider this. Using steganography, a secret can be concealed in a totally innocuous looking file. Only the individual who encodes the secret in the file can decode it and extract what is hidden inside. Unlike cryptography, where the secret is concealed in a jumble of letters and numbers that at the very least suggests something is hidden, the very presence of a secret concealed using steganography cannot be discerned. In fact, it is the perfect cloak of invisibility.

A cloak of invisibility

Using steganography as a cloak of invisibility is extremely handy whether you are intent on getting malware into a protected network or smuggling high-value data out. As long as the cyber criminal chooses an appropriately ubiquitous and easy to manipulate file format in which to encode their secret, they can conceal pretty much anything without needing to concern themself with the threat of being detected.

There are a number of possible file types that lend themselves to exploitation in this way, and right now image file formats are the chosen carriers. It is not hard to see why. Images abound in the online world. Social media is image-driven. The average web page has nearly tripled in size since 2010, and two-thirds of any given page comprises images. Images pass back and forth across network security boundaries every minute of the day.

Not only are images ubiquitous, but the file formats that render them can be easily manipulated using scripting languages and

subtle changes to the content go largely unnoticed. As an example, hidden content can be encoded in the pixels of an image using subtly different shades of colour – invisible to the naked eye – that when decoded might reveal an entire customer database. All in all, images are an ideal carrier.

Poison pixels

Steganography is nothing new. What is new is the adoption of this technology as a concealment technique by cyber criminals to infiltrate malware across the security boundary, to steal high-value data assets and to mask the command and control (CnC) channels into and out of a protected network. In August 2018, a GE employee was arrested after it was discovered he had concealed trade secret information in images using steganography and sent it via email to his personal email account. For over a year now, researchers at GeoEdge have noted the possibility that increasing numbers of online ads containing images could also potentially contain malware concealed using steganography. Deep Secure recently concluded that 50 images posted on social media were sufficient to leak 300,000 credit card details concealed in the image pixels using steganography.

The elephant in the room

For those looking to defend a protected network, image steganography is not only impossible to detect with the naked eye (could you really tell one shade of sky blue from another subtly different one?) but also capable of evading conventional cyber security systems with ease.

Indeed, the uncomfortable truth about this technique is that conventional cyber security defences – firewalls, anti-virus scanners and data loss tools – are all ineffective at dealing with the problem. Any tool that relies on previously seen malware signatures or behavioural patterns cannot reliably detect exploits encoded by way of, for example, pixel transparency. Equally, access to social media tools such as Twitter and to most public websites is unlikely to be prohibited by most organisations.

Of course, some fairly amateurish types of concealment using steganography can be detected, albeit at the expense of a lot of false alarms, but the professional cyber criminal is using image steganography in a way that is essentially undetectable, completely invisible both to the eye and to analysis. Cyber criminals who target organisations in this way can relax in the knowledge that they can effectively operate with impunity.

Beyond detection

The emergence of steganography as a concealment technique undermines the fundamental principle of detection on which all cyber security defence technologies have been based for the last 25 years. Put simply, how can you combat something you cannot detect?

You can employ some basic hygiene precautions to try and limit the threat. For example, if your network allows the use of social media, it will pay to keep it well away from sensitive data and systems. However, the most important step to take is to start thinking that detection is not the answer to this particular problem. Don't try to detect image steganography. Instead, look to employ a defence that will eliminate the places it hides in by removing or replacing redundant data in images.

Transform your defence

In March 2018, industry analyst Gartner published a finding entitled 'Beyond Detection: 5 Core Security Patterns to Prevent Highly Evasive Attacks'. In the report, the author drew attention to Content Transform as key to building defences that deal with threats like image steganography.

Deep Secure uses Content Transform in its Content Threat Removal platform to extract only the necessary business information from images crossing the network boundary. The data carrying the information is discarded, so redundant data is removed or replaced along with any threat. Brand-new images are then created and delivered to the user. Every image crossing the network boundary is automatically transformed in this way, ensuring the threat of exploits concealed in images using steganography is totally nullified.

Content Transform is a way to get and stay ahead of the attacker because it does not rely on detection, on the presence of indicators of previously seen exploits. With attackers adopting ever more evasive concealment techniques like image steganography, it has never been more important to re-evaluate and ask yourself how best to transform your defence.