Anti-virus defences are leaving global businesses vulnerable to the China syndrome

By Greg Sim, CEO, Glasswall Solutions

The news that the China-based APT10 hackers have so devastatingly penetrated the cyber defences of some of the world's biggest commercial and governmental organisations reveals a sickening reality.

Described in a new report from PwC UK and BAE Systems as a sustained, "global operation of unprecedented size and scale", APT10's Operation Cloud Hopper has stolen high volumes of intellectual property and sensitive data from some of the world's major businesses by targeting managed services providers and staging direct assaults on Japanese organisations and companies.

The unpalatable truth behind these revelations is that Operation Cloud Hopper could all have been prevented if these organisations had the right email security technology. By putting their faith entirely in the failed anti-virus solutions touted by the big cyber security vendors, they have left themselves wide open to a new breed of attack.

The report is damning in its revelation that the standard "compromise methodology" used by APT10 was a simple spear phishing email with a malicious "executable" attachment. Using meticulously-acquired data, the emails masquerade as messages from a public sector entity, such as the Japan International Cooperation Agency, for example, while the attachments are crafted to address a topic of direct relevance to the recipient.

For most employees, clicking open such an attachment will be virtually automatic, activating the code hidden in the structure or content of the file attachment. This sophisticated malware immediately rips through networks, heading for the plans, the designs and the data that these incredibly well-resourced threat-actors want to steal.

The sickening reality in all this is that traditional anti-virus protection relied on by the world's major companies and organisations cannot protect them from these attacks. These solutions are not only incapable of detecting 100 per cent of the viruses out there, they cannot detect the sophisticated threats that hackers such as APT10 now deploy inside the instruments essential to everyday business – email attachments.

Consider this simple point. Anti-virus technology relies on identifying the signature of each piece of malware. This means that an attack has to be mounted before the signature can be identified. Yet even though, as the report details, the activities of APT10 and its malware variants have been well-documented since 2009, these China-based hackers still got through.

The report exposes how APT10 malware has been charted right back to when the group was first found to be targeting Western defence companies eight years ago and then on through its variants such as Poison Ivy, PlugX, Quasar, EvilGrab and more recently the development of the bespoke ChChes and RedLeaves.

Yet despite having all this threat-information at their fingertips, the anti-virus companies have still been hopelessly inadequate in protecting major clients. While they look for another name to give to an updated version of the malware, it has been easy for APT10 to escalate its attacks with its cleverly-crafted decoy emails.

Its selection of managed service providers (MSPs) supplying all kinds of IT services to major clients, is also cunning, if not unexpected. MSPs often have systems that overlap with their clients, offering ready access to entire supply chains and all their data. Once its malware is inside a network, APT10 moves laterally between MSPs and other victims and uses a sophisticated pathway to exfiltrate the data is has stolen, leaving minimal traces.

Now many of the victim-businesses that relied on anti-virus defences will find that vital intellectual property is sitting on a competitor's desk in China.

Operation Cloud Hopper makes it clearer than ever that organisations are leaving themselves vulnerable to attack by relying on leaky old anti-virus defences that are incapable of detecting the lethal threats hidden inside either the content or structures of common file types.

When the anti-virus companies admit that they can only protect against 95 per cent of *known malware*, let alone the admission that they cannot stop a zero-day attack, all businesses and organisations must adopt more innovative solutions such as file-regeneration technology that addresses *today's and tomorrow's threats,* instead of searching for what was a threat yesterday.

These are solutions that act as impenetrable barriers, keeping out 100 per cent of malicious exploits in file attachments such as Word, Excel, PDF or PowerPoint. All of these documents have a design standard against which every attachment can be measured in milliseconds, ensuring only the authentic and known good is permitted inside an organisation according to its established risk policy, and without disrupting normal operations.

Glasswall have repeatedly warned against relying on outdated methods to secure borders and specifically document attacks, there has to be a 'new baseline' established to plug the gaping holes that current security has. If the globe's major organisations continue to ignore this technology and rely on anti-virus defences, the alternative is yet more disasters such as Operation Cloud Hopper.

Enquiries: sales@glasswallsolutions.com
Sales: +44 203 814 3900
Website: www.glasswallsolutions.com

-Ends-