Parcel bomb: Some of the biggest security breaches start with an email

Special delivery

Financial institutions need to be ever more alert to suspicious packages coming through the digital mailbox. **João Gouveia**, **Rui Serra** and **José Ferreira** discuss how **AnubisNetworks** is creating a safer business environment by using threat intelligence to intercept them

Cybercrime is an underworld growth industry with few equals. It's been described as 'the greatest threat to every profession, every industry, every company in the world'; and in July 2017 Lloyd's of London warned that a major attack could be more damaging to the global economy than natural disasters such as Hurricane Irma.

João Gouveia, chief technology officer and co-founder of AnubisNetworks, shares this concern and is in no doubt that every organisation is at risk.

"Cybercriminals are constantly finding new ways to infiltrate systems and compromise security, so our challenge is to keep up with ever more inventive types of phishing and malware," he says.

For banks and other financial services companies, though, it's very much a double challenge because not only must they provide secure systems for their customers, they must also help their customers avoid being duped by fraudsters. That's why they need the combined power of a good threat intelligence solution and a good mail protection service (MPS),"Gouveia adds.

He highlights the rise of spear phishing, but points out that it can't be beaten by technology alone.

"Spear phishing is email-spoofing that appears to be from a known contact, and it's very hard to defeat with technology," says Gouveia. "These attacks exploit social susceptibilities. The perpetrators research their targets and get to know them very well, so when they send something, the receiver thinks it's coming from a legitimate and trusted source."

Raising a red flag

Sensitising staff to rogue emails through training is an important part of a business's counter offensive, but for its part, AnubisNetworks uses machine learning to identify and highlight potential intruders, rather than ambushing them before they arrive.

"We implement standards and best practices that ensure we can authenticate email messages that enter a customer mailbox," explains the company's email security expert José Ferreira. "We use sender policy framework (SPF); domain keys identified mail (DKIM); and domain-based message authentication, reporting and conformance (DMARC).

"We try to alert the user if a message looks suspicious. It's not about outright blocking messages because sometimes that causes a false positive," adds Ferreira. "We apply a warning tag that says it may be a spoof message, so proceed with caution. This helps to educate users because they learn to be wary. By setting DKIM on your domain name servers, you're providing a way to tell your receivers that the sender is genuine."

Gouveia emphasises the importance of using technology to stay one step ahead of cybercriminals.

"This is particularly the case when the social component isn't significant," he says. "While a well-conducted spear phishing attack is difficult to block, traditional phishing campaigns, malware and spam can be overcome with technology. Malware, however, is now a big concern because antivirus software is not as effective as it used to be, so that's an area that we're focussing on."

There are several ways to detect malicious messages, some of which use AnubisNetworks' inappropriate fingerprinting algorithms, fingerprinting in this case being a procedure that uniquely identifies an original data file. Once a data fingerprint has been flagged as coming from an untrustworthy source, AnubisNetworks can leverage information in its wider threat intelligence ecosystem to track where it appears next.

"By knowing the fingerprint, we can block it across everyone else that receives the same, or similar, messages," says Ferreira. "Another method, long established in the industry, relates to IP reputation. If you notice that certain devices are constantly trying to send malicious email messages to people, you can track them and block them fairly easily."

Tracking the bad guys

AnubisNetworks strength is enhanced by its being part of, and providing intelligence to, a wider security network.

It's a reciprocal relationship in which the intelligence ecosystem on which MPS is based in turn enhances detection and avoidance of the latest and most advanced threats for AnubisNetworks' own customers. It also enables companies to gain an insight into the security of third parties as well as their own organisation – and in a world where longtail supply chains can quickly be compromised by hackers, such due diligence is becoming vital to good governance.

People are starting to understand the implications of third-party risk following a number of highly public and damaging breaches, says AnubisNetworks product manager Rui Serra.

"Third-party risk management will become increasingly important. Just think of the US retailer Target. In 2013 it was hit by a breach that exposed the data of millions of customers," he says.

Still the biggest reported incident of its kind, Target was hit after its network credentials were stolen from a refrigeration, heating and air conditioning subcontractor.

Gouveia describes the development of the intelligence ecosystem as 'one of the most exciting developments in our industry… because risk inevitably spreads across the business chain. If you're concerned about the protection of your data, you also need to be concerned about data held by your contacts and partners."

Trust and identity

AnubisNetworks supported the principles of the European General Data Protection Regulation (GDPR), due to be introduced in May 2018, long before the law was adopted by the European Parliament, and it is already fully GDPR compliant. That said, it believes the new rules pose some contradictions that frustrate rather than promote efforts to improve security.

For example, currently when a domain is registered, the personal data associated with it is currently freely available; that information is critical to identifying relationships between domains.

"If a domain has tried, somehow, to abuse the system and we know the same person has registered another domain, it probably has the same purpose," explains Gouveia. "So we might use that information to create, for instance, blacklists of domains, that are known to be used by bad actors."

> "If you're concerned about the protection of your data, you also need to be concerned about data held by your contacts and partners

That personal information, however, is likely to disappear under the GDPR, which seeks to protect individuals' personal identifiable information (PII).

"So right now, we, as an industry, are trying to lobby to have that data somehow available – perhaps not as the data itself, we just need to know if it has a relationship with another domain," says Gouveia.

That said, GDPR also plays to the company's strengths, adds Serra, because both set out to build trust and clarity. Financial institutions have a huge responsibility for the way they communicate, particularly over email, and their customers need to be confident that their personal details are always handled sensitively and carefully, and that messages are authenticated.

"Because we help companies understand their current exposure, we support data protection and regulation from all sides," adds Serra. "You need to figure out how you're seen from an external perspective, how others see your data and whether there is a risk factor. Reconnaissance is step one, and step two is reaction."

A robust combination

The threat intelligence ecosystem and AnubisNetworks' MPS work together to deliver a high level of defence against ransomware, spam, business email compromise (BEC), spoofing and phishing.

"We provide a business environment that enables you to detect and avoid the latest and most advanced threats," says Serra, who adds that the company's commitment to reporting and forensics means 'every email on the platform, every transaction, every user and action is rigorously logged and updated'.

Its data scientists are continually investigating new dangers, too.

"Our research team does a lot of work around botnets and how they behave," says Gouveia. "If malware is sent through email, they try to use compromised accounts. We track this at the MPS level for such things as distributed denial-of-service (DDoS) attacks, and we use the threat intelligence database to help decide if a message should be rejected. It's a good example of how MPS and threat intelligence work in tandem."

Managing risk via Cloud technologies, such as AnubisNetworks' MPS is becoming increasingly important in financial services.

"We've been using the Cloud for a long time – in fact, we were one of the first companies to provide a Cloud solution and banks are starting to accept Cloud-based security," says Gouveia.

"Banks like us because our platform has depth of analysis, auditing abilities and a wide range of technology defences all in one," he adds. "With AnubisNetworks, it's strength in combination."