Aaron Higbee

New developments in the war on phishing

Cyber attacks through the technique of phishing rely on human error to be effective and it is through training its own people that an organisation can best protect itself and its data, as defence writer Mark Lane discovers talking to Aaron Higbee of PhishMe.

A cyber espionage campaign has targeted Android smartphones used by Israeli soldiers to gather information such as calls, texts, web browsing and photo files. Two separate research papers, from Kaspersky Lab and Lookout, reveal that more than 100 Israeli military personnel have been targeted in the operation since mid-2016.

The unknown hackers behind the operation use the technique known as 'phishing', attempting to gather personal information by posing as a trustworthy email correspondent. In this case they have used sexual advances from fake female social media profiles to encourage military personnel to click malware-ridden links to spread an exploit now dubbed 'ViperRat'.

The targets included servicemen of different ranks serving around the Gaza strip, with the aim of stealing military data, including location and tactics.

This comes as no surprise to Aaron Higbee, co-founder and Chief Technology Officer of US company PhishMe, a provider of phishing defence solutions.

He says: *"One of the main points for me is that this wasn't an exploit [software designed to take advantage of a flaw in a computer system] against Android or any vulnerability in Android, it was just these soldiers installing an application that had too many permissions."*

PhishMe's business is to make companies and organisations aware of the human element in cyber attacks, so that users recognise and react appropriately to phishing.

"We are a company that helps businesses avoid compromise from phishing or social engineering attacks by offering a service that allows them to send phishing emails to their employees at work; then, if they click on it, they're funnelled to training but when employees receive a suspicious message they can also report it," he explains.

"We send millions of phishing emails and social engineering emails to people at work every year. We feel that this is currently the best way to help organisations ward off phishing attacks."

Phishing may enable the use of malware, ransomware or viruses once a victim or employee of a victim company has clicked on a link or attachment, but the process of persuading them to do that is not down to technology but psychology. This is where the key to an effective defence lies.

"We've had a phishing problem now for over 15 years and technology alone hasn't been able to solve it," says Higbee. *"At the core of this is a human behaviour problem and organisations should ask themselves what they are doing about that."*

PhishMe obtained and analysed the phishing technique that was used to penetrate the emails of the Democratic National Committee during the recent US presidential primaries campaign and then phished its own employees using the same tactics.

Higbee notes: *"Even though we're experts and we do this all day, we still had two employees click it and potentially get infected; but it was, of course, simulated."*

He explains the mechanics of how this was done.

"Because we are a multinational, every year we try to get the company together in a nice warm location and so in our job descriptions it talked about going to Cancun. Right before the Cancun trip our employees received a phishing email warning them about the Zika mosquito virus in Cancun and with a link to click to find out how to avoid it. So we used social engineering, we used fear and curiosity – emotions to get people to click."

In the past, organisations which fell victim to phishing tended not to advertise the fact, unless they were regulated in such a way that they had to disclose a breach.

"It's embarrassing and it's frustrating because you are spending hundreds of thousands of dollars on cyber security products and then an employee clicks a link or emails something they weren't supposed to," says Higbee. *"It's an embarrassment, but it's one people are more willing to talk about as these high-profile breaches hit the headlines."*

PhishMe is finding a high demand for its services. Based in Leesburg, Virginia, it was set up in 2011, and now numbers half the Fortune 100 companies among its clients; about fifteen per cent of its clients are governments. Other clients include banks, oil and gas companies and manufacturers. It has opened its second largest office in London and it also has offices in Dubai, Singapore and San Francisco, with different models in different countries depending on their privacy laws.

"We've had a phishing problem now for over 15 years and technology alone hasn't been able to solve it; at the core of this is a human behaviour problem and organisations should ask themselves what they are doing about that"

– Aaron Higbee, co-founder and CTO, PhishMe

"We are hiring, on average, 12 employees a month. Right now, our current headcount is 320 and it will be over 400 by the end of the year," says Higbee.

And what's to stop other people replicating PhishMe's business model and fighting for the same market?

"A lot have tried. We definitely have competitors in the market. We do have intellectual property around a number of our techniques but that doesn't always help, so our main driver is to continue to be leading edge, to be industry experts. We have the best research team around phishing just to stay on top of the attacks to make sure we are constantly updating our product."

Despite the hacking of the US presidential campaign and fears of Russian interference in the politics of other countries through cyber attacks, Higbee finds governments slow to respond to the potential threat.

He explains: *"It seems to me that they lag behind. The first market sector that really adopted our solutions was financials, then energy came on strong. What has been my observation – and I live in the Washington DC area – is that government really works on regulation and check boxes when it comes to security and so they don't necessarily keep up with the modern attacks; they are worried about compliance with regulations that were developed five years ago."*

He believes that in the near future ransomware will become an increasing cyber threat to organisations. Ransomware is malware that infiltrates a victim's computer through phishing and effectively holds their data hostage, by locking the system or threatening to leak the data, unless a ransom is paid.

"This year I think we are going to see a big change in the way that typical ransomware attacks are operated," he cautions. *"Right now, ransomware is through large internet blasts where the attackers don't necessarily know who they are victimising. They don't know the victim's ability to pay and set the ransom fairly low.*

"What I think will happen in the next few months or year is that the hackers will first infect the computer and then spend a little bit more time to figure out if that computer belongs to an individual or a business. Once they find that out, they'll tune the ransom to a higher amount for a business."

The best line protection once an organisation has fallen victim to ransomware is to have good data back-up.

But, as Higbee emphasises, the best first line of defence against phishing and cyber crime lies not in technology but in people, and he has this one last piece of advice for organisations: *"Critically examine the process that you have in place for employees to support suspicious emails because in every case that we simulate, more employees accurately identify and report the phish than fall for it."*

Further Information

For more information, visit:
www.phishme.com