Ransomware, cyber bullying hits SA companies

The ransomware and cyber bullying onslaught is gaining momentum worldwide, and South African businesses are falling victim too, says Fortinet.

Paul Williams, Major Account Manager at Fortinet, says that while high profile hacks may dominate headlines, un-publicised attacks are taking place against individuals and companies all the time. “We are seeing more and more targeted attacks happening locally,” he says.

Williams cites two recent attacks against local companies, where Fortinet was notified in to assist: “In both cases, the ransomware came in via email attachments that looked legitimate to the users who received them. The malware could be hidden in an Excel spreadsheet or docx file, and the only clue that the mail was suspicious would come from analysing the sender address.”

The users opened the attachments and their machines were locked down by the malware. In one case, the attackers wanted a large sum of money transferred to an anonymous account, while in the other, the demand was for slightly lesser amount transferred to an anonymous account.

In these cases, the affected companies had backed up the machines, so they reformatted the affected machines and did not pay the ransom. “If you analyse the mail, you typically find it comes from regions across Africa, Eastern Block Countries or East Asia,” he says.

“In many cases, hackers target a company’s website in order to make demands, or to use the portal as a gateway to the company’s back end systems. These targeted attacks are done for the purposes of espionage, theft and fraud, or to demand a ransom.”

Williams says he is not aware of any company actually paying the ransoms demanded, but that attacks such as these do present a risk for substantial losses and reputational damage, and underline the need for stepped up security and awareness within companies.

“This trend for hackers to make targeted attacks demanding something of the victim extends to cyber bullying,” he notes. “We now see attackers hacking the devices or social media accounts of individuals in order to bribe them or make demands of them.”

Fortinet’s FortiGuard Labs noted in a report last year that ransomware is now also being used in attacks on mobile phones. Among these are **FakeDefend**, disguised as an Anti-Virus application; **Cryptolocker**, disguised as a video downloader; **iCloud ‘Oleg Pliss’ ranswomware**,

which compromised iCloud accounts in combination with some social engineering; and **Simplocker**, in Trojanized applications like a Flash player. The report recommended using reputable mobile Anti-Virus and installing only trusted applications to mitigate these risks.

Williams says mitigating the ransomware risks depends on increased awareness and ensuring that a number of security measures are in place:

· **Securing the company's web site** is crucial, and not always a primary focus area when companies develop their web presence, says Williams. This can leave companies exposed to defacement and attack. "The proper testing must be in place, with an effective web application firewall in place to block SQL injection, cross-site scripting, buffer overflows, file inclusion, cookie poisoning and access through to the enterprise systems."

· **Intelligent email filtering solutions** are important to analyse incoming emails with Identity Based Encryption, block spam and quarantine any mails deemed suspicious, before they reach the mail recipient.

· **Advanced threat protection and intrusion protection** should be in place to support multi-layered security with a combination of NGX, WAF and Sandboxing.

· **Regular backups** of all machines allow the user or company to simply reformat and reload a compromised machine, if necessary. Williams recommends backing up at least weekly or daily depending on the critical nature of the data.

· **User education and Security risk awareness** remains an important element of information security, says Williams. "Companies must make users aware of the risks, particularly if they use public access or mail non-corporate mail accounts and file sharing services for work," he says.

/ENDS.