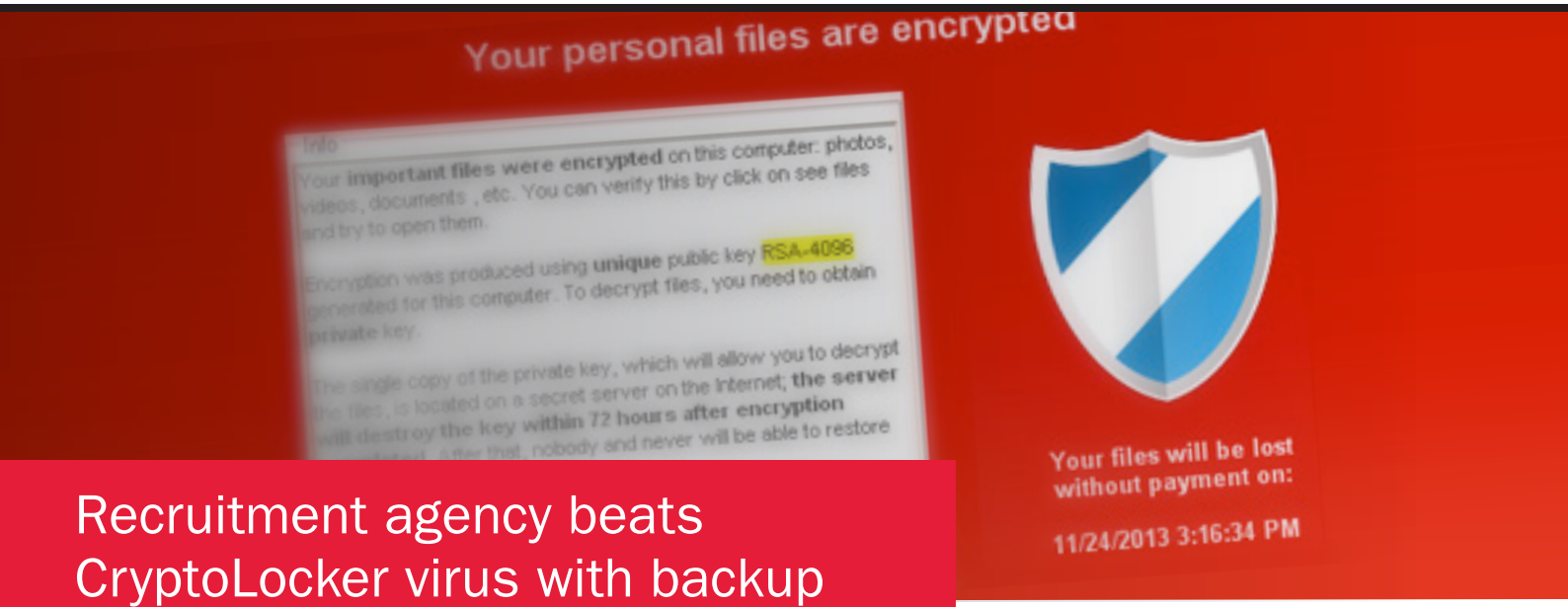
Databarracks

MajorPlayers...



Recruitment agency beats CryptoLocker virus with backup

Major Players is a leading marketing and creative recruitment agency with over 15 years of experience in providing top media organisations and consumer brands with the industry's best and brightest candidates.

Head of IT and Facilities, Jonathan Levene, joined the agency in September 2013, tasked with refurbishing the office interior ahead of plans to grow business throughout 2014.

> "I've got to strike a balance between constantly improving the systems which support our business and ensuring that's done in a financially viable way. The difference with backup from Databarracks is that I know if I've got kit that I don't completely have faith in, we're not going to lose data if the worst should happen.
>
> Jonathan Levene, Head of IT and Facilities

The Challenge

Protecting against viruses and malware is nothing new to Major Players. Spam and malicious emails are just a fact of life for businesses today. Most are identified and mitigated against automatically by whatever security software the business elects to use.

Occasionally, new vulnerabilities and exploits are exposed, but vendors are typically quick to respond with a corresponding quick fix or software update. It's a constant game of cat and mouse that until last year seemed relatively innocuous.

Then came CryptoLocker.

Masquerading as an email attachment often from highly plausible senders, the CryptoLocker virus encrypts both local and shared network file data with a remotely held RSA-2048 key. The victims are then given 72 hours to pay a ransom fee (between 300-400 euros at the time of writing). If the ransom has not been paid after 72 hours, the encryption key is destroyed, and access to those files is lost permanently.

American officials have taken the stance that victims should not pay the ransom, despite the fact that no one is currently capable of breaking the encryption on a commercial scale.

"The nature of our business means that we can't be overly prescriptive with the internet access rights we afford our recruiters. Email correspondence is a critical function for us – it's how the majority of our work is done. Often those mails can be unsolicited."

An estimated 250,000 computers have been affected by the CryptoLocker virus. In most instances, the victims are left with two choices: pay up, or lose the data forever. Jonathan remembers getting the news:

“One day, one of our finance guys came to me saying he had a huge warning message on his monitor with some kind of countdown timer. I instantly knew we’d been hit. Sure enough, when I arrived at his desk I could see the red dialogue box displaying the ransom message and a list of files that were now encrypted and inaccessible.

“We initially considered paying the ransom. The threat isn’t exactly ambiguous, up there in bold on the monitor:

‘...the server will destroy the key after a time specified in this window. After that, nobody can and never will be able to restore files.’

“We decided to contact Databarracks before making any decisions. From the minute he answered the phone, our engineer, Tom, knew exactly what to do. He was unequivocal: ‘don’t pay the ransom, we can get your data back for you.’”

The Solution

“Tom ended up giving us our get out of jail free card. He sent us our files back immediately so we could access them locally and then stopped the daily scheduled backups from running to prevent the encrypted files from overwriting our existing backups.

“It was actually so smooth, no-one in the office even noticed. I’ve seen organisations where backup is a secondary consideration, and it’s situations like this that really demonstrate how important it is to stay on top of things.” - Jonathan Levene, Head of IT and Facilities

“Anyone can be affected by ransomware such as CryptoLocker. Staying up to date with the latest developments is an important starting point. Half the battle is knowing what to look out for; if you recognise a suspicious email as a threat, the whole security incident is avoided. Ultimately though, our message to our customers is to consider good backup practices as both the best defence against and antidote to attacks like this.” - Databarracks Managing Director Peter Groucutt

> “Our message to our customers is to consider good backup practices as both the best defence against and antidote to attacks like this.
>
> Peter Groucutt, Managing Director, Databarracks

Databarracks

Databarracks | **Unit 6** | 9 Park Hill | London SW4 9NS
t: +44 (0) 800 033 6633 e: info@databarracks.com www.databarracks.com