Can Lady Gaga and Madonna get people to take security seriously

Can Lady Gaga and Madonna get people to take security seriously?

Alex Scroxton, Security Editor

The holding to ransom of a business that very few people have ever heard of rarely makes the mid-afternoon news bulletin on BBC Radio 2, but the mainstream media was prepared to make an exception in the case of NYC-based law firm Grubman Shire Meiselas and Sacks, which has been attacked by Gold Southfield, the cyber crime group behind the ReVIL/Sodinokibi ransomware strain. Why might this be?

The facts of this ransomware case are quite mundane. The attack on Grubman's network saw 756GB of documents on multiple clients stolen, including contracts, non-disclosure agreements, phone numbers and email addresses. As is becoming quite normal, the attack bears some hallmarks of a double extortion attempt, as some documents have been posted on a dark web forum as proof that the hack is genuine, and as a threat to encourage the victim to pay up.

It is true that not many people outside the legal profession will have heard of Grubman, but this case is rather more remarkable than usual because those affected by the incident includes a huge roster of celebrities, such as Bette

Midler, Bruce Springsteen, Christina Aguilera, Idina Menzel, Lady Gaga, Madonna, Mariah Carey, Mary J Blige, Nicki Minaj and Run DMC.

The documents posted online, incidentally, are excerpts from a contract for Madonna's recent Madame X tour.

In a statement to showbiz magazine *Variety*, one of the first outlets to report the story, a spokesperson for Grubman said: "We can confirm that we've been victimised by a cyber attack. We have notified our clients and our staff. We have hired the world's experts who specialise in this area, and we are working around the clock to address these matters."

Sam Curry, chief security officer at endpoint protection service Cybereason, is a frequent commentator on the big hacks of the day. He described the attack on Grubman as a "surgical strike", clearly designed to attract global attention.

"Human beings are the single biggest asset that cyber criminals have in extorting money, and specifically in the case of the breach of the Grubman law firm," he said.

"The million-dollar question is how much personal information the hackers have obtained and how real are their threats? And what are the ransom demands of the hackers?"

Curry added: "If the hackers have obtained personal information of these celebrities, will they give Grubman the encryption keys and return stolen files if

the ransom demands are met? Unfortunately, there are no longer any guarantees for companies that decide to pay a ransom."

Hell hath no fury like a celebrity hacked

Francis Gaffney, director of threat intelligence at email security firm Mimecast, said the high-profile nature of the victim's list could mean it will face more trouble down the line as those on the list can afford to "lawyer up".

"When somebody trusts you with such important information, it is vital that you adequately protect it, know exactly where it is stored and who is able to access it," said Gaffney.

"It is also not just the financial penalties that businesses face, but the damage to their reputation as well. Once this happens, brands often lose the trust of consumers and partners, and this can be a struggle to recover. This is particularly relevant in this case, with the data belonging to such high-profile individuals."

Ilia Kolochenko, founder and CEO of web security specialist ImmuniWeb, said such law firms are almost irresistibly vulnerable to cyber criminals.

"Law firms are increasingly becoming desirable targets of sophisticated cyber gangs," he said. "It is often much easier and faster to breach a mid-sized law firm to get ultra-confidential data compared to targeting its large clients directly, such as banks or celebrities, as reportedly happened in this case."

Kolochenko said that, in general, he saw little interest among legal firms in prioritising investment in things that can ward of a ransomware attack before any damage is done, such as basic cyber resilience and defence, staff training, or incident detection and response.

“Worse, modern law firms have to deal with diversified digital flow of sensitive and privileged data on their mobile phone, laptops and office computers,” he said. “Partners and clients exacerbate this convoluted landscape by uploading confidential documents to public cloud or file-sharing websites.”

A rising tide lifts all ships?

There can be no question that the high-profile nature of Grubman’s client list caused ears to prick up beyond the specialist technology press, and public interest in the story is high, but how does that translate into wider security awareness?

A perennial frustration in the industry is that people simply don’t listen to security advice, or consider it and decide either that they can live with the risk, or that it’s too late to do anything about it now.

Are we so cynical as to think that attaching Lady Gaga’s and Madonna’s names to a story will grab people’s attention?

Tim Erlin, vice-president at compliance specialist TripWire, disputes this thesis, at least as far as ransomware is concerned.

"The public imagination isn't really the challenge," he said. "Most of these attacks are perpetrated against businesses, and getting business leaders to change is a key component to success. Celebrity attacks don't generally influence executives."

Jonathan Knudsen, senior security strategist at app security firm Synopsys, said this particular attack highlighted, to some extent, the nature of the news cycle in that when people make bad security decisions, they get caught out, but when they make good ones, nobody cares.

"What happens when system administrators expeditiously patch a vulnerable library or application?" he said. "What happens when applications that are used daily by millions of people don't fail? In many cases, nothing. We tend to only see headlines when something bad happens.

"Even though security professionals might be demoralised by the continuing parade of bad news and unfortunate choices, they should remember that things are also going right – you just won't necessarily hear about it."

But Mimecast's Gaffney takes a slightly different view. "These high-profile attacks do help to 'tell the story' and increase awareness," he said." Being able to offer a case study or example with a person an end-user 'knows' – or can relate to – enforces the cyber security message and updates users on current, prevalent threats. The media coverage facilitates the objectives of awareness training to end-users."

Jérôme Robert, director at active directory security specialist Alsid, said: “It could be tempting to look at this ransomware event affecting a high-flying law firm serving the rich and famous and think that it doesn’t really matter. So what if a few secrets emerge? They are celebrities, so they don’t have much right to privacy anyway, and we might get some juicy details about their lives or legal affairs. Right?

“Wrong. The problem is that privacy has to exist for everyone equally, otherwise it won’t exist for anyone. What about the ‘normal’ people whose data would also be exposed as part of the breach? Celebrities should have a right to privacy like anyone else, not to mention that if the law firm pays the ransom to get its data back, that’s an incentive for cyber criminals which will lead to more ransomware attacks.”

Synopsys’ Knudsen agreed there were valuable lessons for the general public in the Grubman hack. “Like the celebrities whose information is now in jeopardy, we all interact with organisations every day that might result in a situation like this,” he said. “It is impossible to evaluate the security posture of every business where you have sensitive information and, for the most part, we must rely on a system of trust.”

But ultimately in such cases, said Knudsen, consumer security will only ever be as good as the security of whoever holds their data. “Businesses can reduce the risk of a catastrophic breach by taking a proactive, security-first stance and

following industry best practices in designing and implementing their technology solutions," he said.

Clearly, Grubman has been found wanting in this department.

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com