GW GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

Podcast

November 2021

Health Care Podcast Series

Episode 1: No Click Hack Risks - Pegasus Spyware

By: Terence Russo and Philip Hammarberg

Terence Russo: Hello, this is Terence Russo. I am Chair of the Healthcare Information Technology Group at Garfunkel Wild and welcome to the Garfunkel Wild, P.C. Healthcare IT Podcast.

Terence Russo: Today I'm here with Phil Hammarberg, who is head of Garfunkel Wild's Intellectual Property Group and we're here to discuss some of the scary new spyware out there and the zero click hack risk. So Phil thanks for joining today.

Philip Hammarberg: Thank you. So first why don't I start by talking about some background related to smartphone hacking, I guess hacking in general. Most people view hacking as a very high tech process and certainly can be but, generally speaking, most hacking is commonly done by tricking people.

Philip Hammarberg: Tricking people to click links or to download something in order to inject a virus or malware into the IT system or for the purposes of this conversation, a smartphone. It's typically easier for hackers to trick a person than it is for hackers to defeat sophisticated technical safeguards and firewalls.

Terence Russo: The weakest link in my experience is generally the human factor. Humans who fall for social media scams or any phone calls, all sorts of tricks but, this one is a little different isn't it?

Philip Hammarberg: It is. So, a zero click hack or exploit, is sort of the one exception to that rule. A zero click exploit, unlike typical hacks, are generally not preventable until the provider of the software or the smartphone patches it or corrects the software.

Philip Hammarberg: An example of a recent and very concerning zero click exploit was the Pegasus spyware software that was used and directed to iPhones. Pegasus spyware was capable of infecting any iPhone. Until the software was patched by Apple in a way that prevented the spyware.

Terence Russo: I’ve been reading a lot about Pegasus spyware and even saw an article in the journal yesterday. I know it was International maybe developed by Israeli spyware company, but, how long has this been out there, Phil?

Philip Hammarberg: So, based on the publicly available information, it's been out there at least nine months, it could go back a lot longer than that. I think that's when it really started to become public release that they're able to track the spyware back to the Spring of this year.

Terence Russo: Got it. You know it's definitely been in the news a lot recently. I think I even heard of some cases they thought it's been around since 2016 which is kind of scary because I always thought Apple, everyone always told me my Apple iPhone was pretty darn secure.

Philip Hammarberg: That was definitely the common belief and it probably is pretty secure, but even though iPhones were the gold standard of secure smartphones, no security system on IT devices is perfect. There will always be loopholes, exploits, and vulnerabilities that come about, and hackers are working 24/7 to devise new ways to get into IT systems.

Terence Russo: It’s kind of scary. It's a war. You've come up with a better security system and the hacker finds a better way in. So what are some of the takeaways?

Philip Hammarberg: So I think, bringing this back to sort of the healthcare IT space and healthcare IT agreements, I think it's important to ensure that vendors will promptly patch and update their software, the moment that they become aware of these vulnerabilities.

Philip Hammarberg: I also think it's very important to have appropriate warranties and data security terms, so that at least you know that the vendor is using industry best practices.

Philip Hammarberg: And then, finally I think it's really important to have an appropriate limitation of liability based on the type of data, the scope of the data, and how it's being hosted or stored.

Terence Russo: That's my one of my favorite topics: appropriate limitations of liability, just for the listeners out there. You know, sometimes when you click and use an app the vendor’s saying “hey if anything happens and there’s a data breach I’m not liable”, so you have to be aware and that's something that happens. Especially the quick wrap terms and with almost everyone that's actually the default where they try to disclaim all responsibility so in terms of your healthcare system or provider and like everyone else you want to access your electronic health records or medical information. Even using your iPad and people are using iPhones. I know Epic has it out there, all the big vendors have mobile systems out there now.

Terence Russo: Just because you're on your iPhone doesn't mean it's safe. And Phil, one thing I always heard is that iPhones were basically always built-in with standard encryption, robust encryption, did this zero click hack of Pegasus spyware somehow bypass that or how did that work?

Philip Hammarberg: Sure, so they do have great encryption, certainly as good as any other phone that I'm aware of. But unfortunately encryption only works to prevent people from accessing your data when it's encrypted. So when you're on your phone and you unlock the phone, at that moment, the data is unencrypted which is decrypted, at least the data your accessing. And that's actually when the zero click spyware was introduced into people's phones - when they were logged into the phones and so, in that way, it was able to access their decrypted data.

Terence Russo: Very scary. So in terms of Pegasus, in particular, but just to get a sense, even if you're texting, not even sending emails, I heard that this spyware could turn on your microphone but even text, everything was available then to these hackers in what most people, until recently, felt was one of the more secure phones.

Terence Russo: I remember when the FBI was begging Apple to allow it to break into iPhones and Apple was resisting and I was thinking "wow, Apple really is like Fort Knox". I think this goes to show you that no system is really perfect and there's always risk. Not that I want to keep people up at night, but that's why before you use any product, you have to be aware of "Is the vendor putting skin in the game", or are you using it at your own risk? And the general rule is *caveat emptor,* "buyer beware", and when you're paying nothing for something, a free app, especially beware, because very rarely do the vendors in those situations, in my experience, give you any real warranties or assurances. Phil are you finding the same thing?

Philip Hammarberg: Yes, I think that's a very good point. Obviously, if you're getting apps for free, you have very little negotiating leverage.

Terence Russo: Yeah. So some of the takeaways: realize no IT system is perfect and think about something, especially for the health care providers, before you start putting data out there you're dealing with a whole new level of risk, not just talking about your personal emails, you don't want your personal info out there, your credit rating, all that other stuff but you're dealing with patient information through an app.

Terence Russo: You always have to really think it through, because those fines can be significant and Office of Civil Rights (OCR) investigations can be significant and expensive. So, I guess, that's the moral the story - no system is perfect, you really have to be aware of your legal terms and conditions before using them.

Terence Russo: Phil, thank you so much for today and maybe one of our next podcasts we will follow up on some of these appropriate data security terms and appropriate limitations of liability. I think that would be helpful.

Philip Hammarberg: Indeed, thank you.

Terence Russo: Have a good day bye.