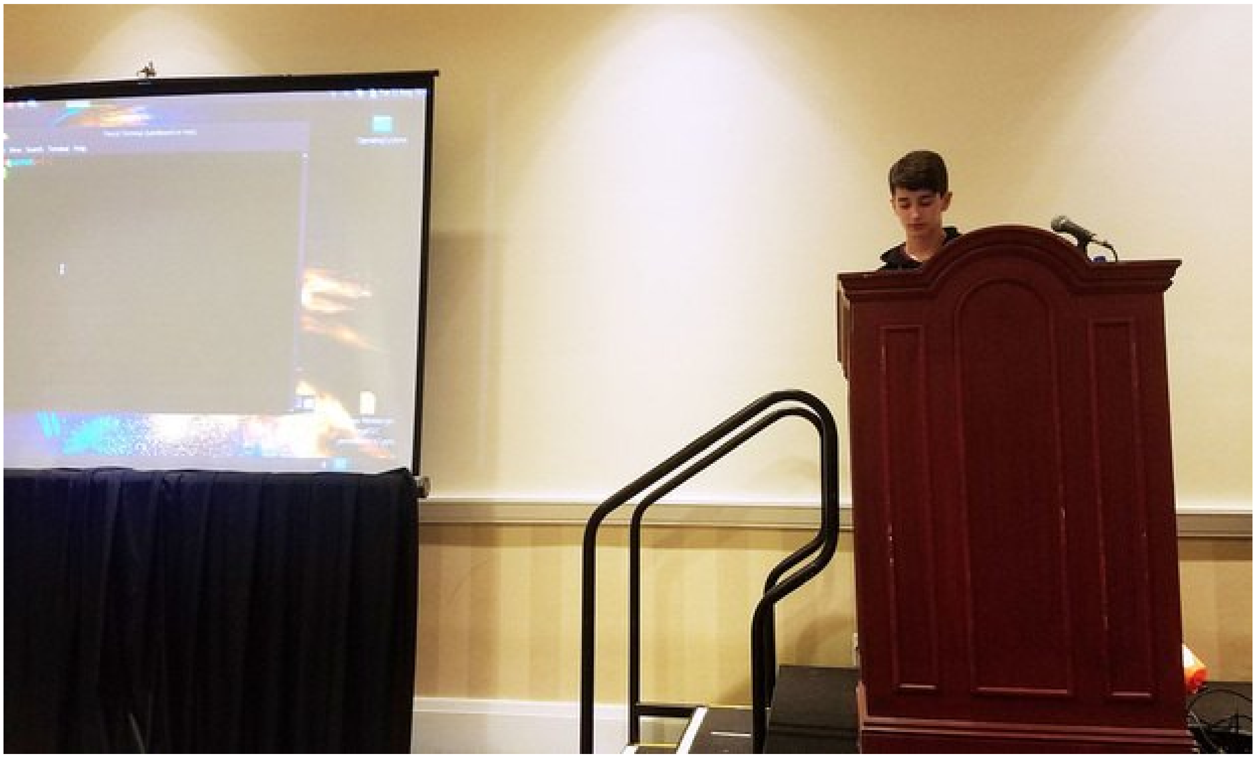
How a Even 15 Year Old Can Hack Your Law Firm

By Stephen Embry



I recently had the chance to attend the annual conferance of the International Legal Technology Association. ILTA refers to itself as a peer to peer networking organization for those in the legal tech field. It describes itself as a “volunteer led, staff managed association with a focus on premiership.” It is primarily made up of large law firms and better known legal technology vendors. At this year’s conference, for example, there were lots of legal professionals from well known and well heeled law firms, legal start ups and practicing lawyers.

One of the hottest speakers at this year’s Conference was self-taught hacker Marcus Weinberger whose talk was entitled “Watch a 15 Year Old Hack Your Firm’s Users”. Marcus mesmerized the audience by showing just how easy it is to hack law firms and their clients.

If you labored under the illusion that hacking is a difficult, arcane skill that only well-resourced, highly trained attackers can pull off, think again. Weinberger showed us in a matter of minutes by using widely available resources like Google and GitHub, and purchasing a few relatively inexpensive tools, just how easily one can infiltrate a law firm’s web assets and employees.

The real kicker: Marcus is 15 years old, not yet old enough to drive a car in most places. (Given his age, its no surprise that Weinberger was accompanied by his father, Ben Weinberger, who is the lawyer in residence for Prosperoware, an enterprise software company focused on legal and professional services. Ben’s role, as he described it, was mainly to “keep Marcus out of jail” and remind the audiences over and over that “Marcus Weinberger only hacks for purely educational purposes everyone”.)

Some of the equipment Marcus uses to hack and, as he put it, “mess with people on Wifi” goes for as little as $1.50. And as Marcus put it, “This is not the dark web we are talking about here. All tools are all readily available to anyone here.” In fact all the products he showed can be purchased from mainstream sites like Amazon and eBay.

Nor are the tools expensive: the most expensive device demonstrated was a Wifi Pineapple that runs around $50. A Pineapple can basically force your phones to join a network of the hackers choosing and enables a hacker to record your activity and enable diasterous “Man-in-the-middle” attacks.

Just listening to Marcus for a few minutes demonstrated how vulnerable many of us are. For example, Marcus explained how Wi-Fi hacks can trick consumer devices into automatically connecting to a malicious network without the device’s user knowing. Said Master Marcus: “When your phone scans for Wi-Fi it will send out a list of networks it is looking for … and what [hacking] devices do is notice that list and respond, and your phone will automatically connect to those.” By tricking a Wi-Fi network to mimic the name of a common network that devices will likely recognize and connect to, hackers can then comprise many devices, including personal devices used by law firm employees. (Marcus cautioned us all to turn off our WiFi before he started; one unfortunate person didn’t and Marcus found his device with the mere push of a button)

And instead of relying on technical exploits, Weinberger noted that hackers can also trick users into infecting their own computers with malware by executing automated phishing attacks. Another tool he found and showed us will send a Twitter user “a direct tweet from an account they are familiar with, and the tweet can include a phishing URL” that mimics a well-known link, but is really a malicious link. All the hacker then needs to do is create a fake Twitter account and get followed by some of their targets.

Marcus showed us how websites vulnerable to hack attacks can be identified through simple Google searches. With a vulnerable site and the help of massive password dictionaries, breaking into a site is then no problem.

And hackers also creat convincing fake sites — often by registering domains that *look* like established firms but actually have non-English characters in the name that appear to be English characters. For example, Cyrillic letters look almost identical to standard English characters.

But hackers don't stop there; when someone tries to log into the fake site, their password to access the real site won’t work. Once given a message that the password isn’t valid, though, Weinberger says that many of us start rolling through all our alternative passwords for other sites — getting each recorded by the hacker who is now has multiple username/password combinations.

The presentation was a scary reminder that none of us are truly safe. Of course, Marcus hacks for good, identifying weakness for companies and then helping them fix them. But others aren’t.

By the way, if there’s one tool outlined in this presentation that everyone should use, it’s a routine check of Have I Been Pwned. This website tells you if your email has ever been compromised. Want to learn something scary; enter your firm email addresses or for that matter the email addresses for some well-known attorneys. I’ll warn you, you won’t like what you see.