You Can Get Hacked Just By Watching This Cat Video on YouTube

15. August 2014

Morgan Marquis-Boire, The Intercept

Many otherwise well-informed people think they have to do something wrong, or stupid, or insecure to get hacked - like clicking on the wrong attachments, or browsing malicious websites. People also think that the NSA and its international partners are the only ones who have turned the internet into a militarized zone. But according to research I am releasing today at the Citizen Lab at the University of Toronto's Munk School of Global Affairs, many of these commonly held beliefs are not necessarily true. The only thing you need to do to render your computer's secrets - your private conversations, banking information, photographs - transparent to prying eyes is watch a cute cat video on YouTube, and catch the interest of a nation-state or law enforcement agency that has $1 million or so to spare.

To understand why, you have to realize that even in today's increasingly security-conscious internet, much of the traffic is still unencrypted. You might be surprised to learn that even popular sites that advertise their use of encryption frequently still serve some unencrypted content or advertisements. While people now recognize that unencrypted traffic can be monitored, they may not recognize that it also serves as a direct path into compromising their computers.

Companies such as Hacking Team and FinFisher sell devices called "network injection appliances." These are racks of physical machines deployed inside internet service providers around the world, which allow for the simple exploitation of targets. In order to do this, they inject malicious content into people's everyday internet browsing traffic. One way that Hacking Team accomplishes this is by taking advantage of unencrypted YouTube video streams to compromise users. The Hacking Team device targets a user, waits for that user to watch a YouTube clip like the one above, and intercepts that traffic and replaces it with malicious code that gives the operator total control over the target's computer without his or her knowledge. The machine also exploits Microsoft's login.live.com web site in the same manner.

Fortunately for their users, both Google and Microsoft were responsive when alerted that commercial tools were being used to exploit their services, and have taken steps to close the vulnerability by encrypting all targeted traffic. There are, however, many other vectors for companies like Hacking Team and FinFisher to exploit.

In today's internet, there are few excuses for any company to serve content unencrypted. Any unencrypted traffic can be maliciously tampered with in a manner that is invisible to the average user. The only way to solve this problem is for web providers to offer fully encrypted services.

Last year, my colleagues at the Citizen Lab and I released a paper on the commercialization of digital spying and the burgeoning third-party online-surveillance market. Historically, this technology has been the province of nation-states with the capacity to develop their own boutique capability. Targeted online surveillance typically involves a software "implant" surreptitiously installed on a user's machine allowing complete control of, for instance, a mobile

device or laptop. Intelligence agencies in the U.S., U.K., Russia, Israel, China, etc. have developed their own custom versions of these. But over the last five years, Hacking Team and other players have begun selling this type of capability for what could be considered “dictator pocket change.” Nations who lack the ability to create their own tools can now accelerate their online targeted surveillance programs relatively cheaply.

These so-called “lawful intercept” products sold by Hacking Team and FinFisher can be purchased for as little as $1 million (or less) by law enforcement and governments around the world. They have been used against political targets including Bahrain Watch, citizen journalists Mamfakinch in Morocco, human rights activist Ahmed Mansoor in the UAE, and ESAT, a U.S.-based news service focusing on Ethiopia. Both Hacking Team and FinFisher claim that they only sell to governments, but recently leaked documents appear to show that FinFisher has sold to at least one private security company.

It is important to note what I’m describing today is not massive intercept technology (although it can be used at scale). Unlike the NSA’s metadata collection, these tools are not used to target entire nations. Nevertheless, we need to have an open discussion about how we want law enforcement using this type of technology. Is it being used to catch child pornographers? Kidnappers? Drug dealers? Tax cheats? Journalists who receive leaked documents?

In the digital age, a search through the contents of your laptop, online accounts, and digital communications is just as invasive as a search of your bedroom. Historically, being privy to someone’s most intimate moments and conversations would once have required placing bugging devices inside their home, not to mention the time and manpower to listen to what was being captured. The cost of such an operation required the target to be someone of reasonable interest. Now, it’s possible to watch someone through the lens of their laptop’s camera, to listen to them through the microphone of their cell phone, and to read through online correspondence cheaply and remotely. The canonical surveillance van full of bored government employees (being paid overtime) deployed 24 hours a day is increasingly a thing of the past.

We simply don’t know how often this type of surveillance occurs. While the Snowden revelations of the last year have revealed much about the character of surveillance by the intelligence community, the use of hacking for law enforcement surveillance is less well understood. There is widespread agreement that law enforcement techniques should be held to a high standard of transparency. Indeed, in the U.S., law enforcement agencies publish records detailing the number of wiretaps they deploy each year. But there is almost no public information on law enforcement hacking.

As the costs of deploying this type of technology decrease, and the tools become commercialized, their use is growing much faster than is commonly understood. The research I am publishing today tries to move our understanding forward, but ultimately the answers as to how to respond are going to come from informed dialogue. Each country needs to have an open discussion about which law enforcement agencies should be authorized to use this technology, under what circumstances, and how oversight should to be updated to accommodate this new capability.