The Hacking Team Data Breach in a Nutshell

by Brian Roux - Wednesday, July 29, 2015

http://hanrylaw.com/2015/07/29/the-hacking-team-data-breach-in-a-nutshell/

I wrote briefly about the Hacking Team Data Breach yesterday in the context of data breaches generally. This is an interesting area of the law because of all the high profile breaches in the last couple of years, the upsurge in interest in cyber liability insurance products, and increasing numbers of regulatory regimes both domestically and abroad. The Sedona Conference Working Group 11 is in the process of drafting a number of documents related to all of this, so the Hacking Team breach occurs at an interesting time. This blog post is going to split into three points: (1) What was/is "Hacking Team"; (2) What was breached?; (3) What is the potential impact short and long term.

Hacking Team

Hacking Team is a company in Milan, Italy that produces a suite of tools for surveilling computers, internet communications, mobile communications, etc. Many people are familiar with remote access tool that include some old hat capabilities like key logging, screen grabbing, communication (email, instant messages, web browsing) interception etc. You can find these kinds of products all over the internet especially marketed towards the divorce and/or cheating spouses market. Those commodity commercial tools can be nasty to detect and get rid of, but are usually installed manually by the other spouse.

Hacking Team produces a product called "Remote Control System" with the current version named "Galileo". They literally advertise their product as "The Hacking Suite for Governmental Interception" in a super creepy Orwellian promotional video. The system uses a number of techniques, including 0day exploits, to infect computer and cellphones in order to carry out pervasive intelligence gathering. These capabilities have been written about and criticized for a number of years. (See Bruce Schneier, "More on Hacking Team's Government Spying Software", https://www.schneier.com/blog/archives/2014/06/more_on_hacking.html; Also see Morgan Marquis-Boire et al, "Police Story: Hacking Team's Government Surveillance Malware", https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/).

Keeping with the theme of aiming this article at the lawyer/laymen community, I'll tl;dr this. Hacking Team is a company that produces advanced malware for espionage and domestic intelligence operations. That malware is very advanced, and its customer base includes state actors. These are not the kind of people the Internet has warm fuzzy feelings about.

(Author's note: I have a tendency to anthropomorphize the Internet when referring to the various communities, consensus, social media collective phenomenon that is, essentially, a global discussion and consensus opinion building.)

What was breached?

Sometime between July 5th-6th a breach was announced over the hacked twitter account of Hacking Team (See https://web.archive.org/web/20150706010312/https:/twitter.com/hackingteam). Contemporaneously, approximately 400GB of data was released via bittorrent. That is a LOT of data. The total corpus is still be downloaded and analyzed by experts across the world, but we do have some interesting bits that are coming to light.

Invoice and Sales information was breached showing Hacking Team's customer base. Hacking Team publically claims they maintain a high road approach to who they will sell to, including substantial vetting processes to avoid selling to, inter alia, states that would use it to "facilitate gross human rights abuses" or violate blacklists produced by the, "U.S., E.U., U.N., NATO or ASEAN". (See "Customer Policy", http://www.hackingteam.it/index.php/customer-policy). Despite this, they appear to sell their technology to a number of questionable state actors including Sudan. (See Steve Ragan, "Hacking Team hacked, attackers claim 400GB in dumped data", http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html (discussing an invoice to Sudan for 480,000 euros)).

Source Code was breached. The source code for their "Remote Control System" was part of the breach. They initially denied the extent of the breach, but later acknowledged it in a news release. (See "Information related to the attacks on HackingTeam on July6, 2015", http://hackingteam.it/index.php/about-us, retrieved 2015-07-08 ("**HackingTeam's investigation has determined that sufficient code was released to permit anyone to deploy the software against any target of their choice.**")). Included in this code were software exploits that allow malicious actors to compromise computer systems. One such exploit was an 0day for Adobe Flash player. (See CVE-2015-5119, https://helpx.adobe.com/security/products/flash-player/apsa15-03.html). This impacts all major browsers because it is an attack against the adobe flash plugin, a fairly ubiquitous piece of software, and there are already reports of its exploitation in the wild. (See Swati Khandelwal, "Zero-Day Flash Player Exploit Disclosed in 'Hacking Team' Data Dump", http://thehackernews.com/2015/07/flash-zero-day-vulnerability.html).

tl;dr – A very sophisticated security tool previously sold exclusively to governments had its source code leaked along with computer exploits that were previously undisclosed and pervasive. Those exploits are now accessible to anyone across the globe to potentially compromise any system at least for the time being.

More to come. Analysis of the corpus is just beginning as researchers across the globe pour over it. Much more is sure to surface in the next few days.

Potential Impact

Short term. At least in the short term, there are wide spread sophisticated exploits now widely available for any malicious actor to use along with a sophisticated espionage tool. It is not hyperbolic to say this includes very bad actors like terrorist organizations as well as bad state actors who may previously have been denied sales of the software. Because patching takes time, and many systems will go unpatched for significant periods of time, these threats will persist for some time into the future. The exploit has already made it into a module for the popular metasploit framework. (See "Adobe Flash Player ByteArray Use

After Free", https://www.rapid7.com/db/modules/exploit/multi/browser/adobe_flash_hacking_team_uaf).

Concerning coincidences. There are also concerning high profile technical glitches occurring contemporaneously with this breach including the halting of trading on the New York Stock Exchange (See "New York Stock Exchange Suspends trading", http://money.cnn.com/2015/07/08/investing/nyse-suspends-trading/index.html), United Airlines grounding all of its airlines, (See Chris Isidore et al, "United flights resume after computer problem", http://money.cnn.com/2015/07/08/news/companies/united-flights-grounded-computer/) , and a number of other odd failures of modern technology (See "Ladies and Gentlemen, It's Time to Panice", http://gawker.com/ladies-and-gentlemen-its-time-to-panic-1716514222). As I said, unless this is confirmed to be from a cyberattack, these are likely to be coincidental, but because of the potential scope of the Hacking Team data breach every such coincidental failure will have to be scrutinized as a potential intentional act. The NYSE took to twitter to update everyone disclaiming it as a cyber breach, but that also means they investigated it for the potential to be one. (See "New York Stock Exchange trading halt 'not result of cyber breach'", http://www.nola.com/business/index.ssf/2015/07/nyse_trading_not_cyber_breach.html#incart_river).

Long term. Long term impact is less clear. The exploits themselves will be patched as the research goes on, but the source code breach will almost certainly advance malware in the future as authors adopt detection avoidance techniques the Hacking Team software utilized. The RCS software may itself, and likely will, be converted and adapted into new malware turning it from a surveillance tool into ransomware or even potentially a launching point for more sophisticated cyber attacks.

Final Thoughts

This story will continue to unfold both as analysis continues of the breached data and as malicious actors begin using what was dumped. Hacking Team is in a lot of trouble. As their customer and sales records are pursued, their involvement with certain state actors is almost certain to result in a PR nightmare. From an ethical and moral standpoint, there are serious questions about their culpability in providing these tools to such state actors especially if those actors have histories of human rights violations and where those tools are used to further human rights violations. We will also see analysis of email in the future shedding light on other projects they may have been proposing, working on, or otherwise involved with and names named for the companies and countries that were party to it.
