RISK ASSESSMENT

Omar Salih

12285240

2.1.2017

As discussed in the article on HelpNetSecurity, ContextIS researchers discovered some vulnerabilities that allows remote hackers to attack a Samsung Galaxy device that will go into a never ending loop of rebooting if a ransom note gets ignored. If the ransom is paid then, the attacker will send another sms message to stop the rebooting of the phone. If the owner of the phone doesn't pay the ransom then the phone will continuously reboot, unless the owner of the phone does a factory reset, which will wipe out everything on the phone, meaning that all information stored on that phone will be lost.

So the attacker initially send a sms message that states that if you pay, then your phone will not be disturbed. Otherwise, if you ignore the sms, then another sms is sent that will make the Samsung Galaxy go into a crash and boot infinite loop. So once that happens if the person pays up, then another sms is sent to stop the loop from happening anymore. This attack uses the vulnerabilities that are caused by Samsung's modified Android telephony framework of CVE-2016-7988 and CVE-2016-7889 thru SMS on the older S4, S4 Mini, S5, and Note 4, but also on the newer S6 and S7 models after the modification was made. Now even though you have updated your phone, there is a malicious application that abuses the CVE-2016-7988. The main issue falls on the face that the modified Android telephony framework that are found on Samsung specific application for handling the carrier messages. They were patched on November 2016.

This shows that these vulnerabilities can give access to individuals that shouldn't have access to sensitive information or even national security vulnerability. Sensitive information can end up in the hands of individuals that can in turn use this vulnerability to attack the individual, the individuals business, personal security, and general public security as well. Samsung left very wide open door to allow attackers access to personal and private information, and allows the attackers to threaten and hold individuals hostage until they comply to the attackers demands or face losing everything they have worked on up to that point. Shows that Samsung didn't notice or think about of the importance of leaving those modifications left as such. This shows that security wasn't on their top priority.

These issues can be very impactful on the individuals that do business on these devices. Wiping out all the data on a phone can be very debilitating to a person that doesn't have all their business documents backed up somewhere besides the device in question. The phone can be damaged by it constantly being rebooted and the data itself can get corrupt causing both to be lost permanently. Samsung once notified about the issue then they corrected the vulnerability, but we don't know for sure if all the users got the patch or no, due to the Android OS update model. But if the said person that got one of these attacks is an employee of a company, and uses this phone for work, then potentially the company or employee would have to pay the attacker or decide to just lose the information on the device. So there

would need to be a measure in the company's security protocols that evaluates the value of data on employee's devices and at what job level is it worth recovering these phones from the attackers or just calling it a loss and resetting the phone back to factory settings. For example, if a company is going thru some big negotiations of deals, mergers, court cases they are dealing with or anything that this said employee might be a part of. Then it may be valuable for them to recover the phone, but lower level employees may not be worth for them to go after the attacker or make a deal with that attacker.

In the short-term the company would need to educate the rest of the company's employees about how to avoid security flaws. Awareness and training, tell all employees to not respond to SMS's that come from unknown contacts. Make sure that the employees know to keep the setting on all devices to not accept to download any unknown sources. Also, they should know not to download any software that they aren't 100% sure of, or company approved. This should avoid all the issues of running the script that would make the phone crash and reboot infinitely. There would need to be some maintenance on all devices should be updated so that all patches are in place. Also, any instance on any company devices be reported to supervisors or management. There would need to be an incident response as well. A contingency plan needs to be in place if all fails what we would need to do to replace the data on the phone and how do we move forward after the attack. A risk assessment also would need to be conducted to see what the risk of not responding to the ransom is and what would be best action forward.

For the long term, we would need to fix and avoid all issues going forward. The security team at the company would need to keep educating themselves of any new and upcoming hacking possibly that may affect the company. Do a risk assessment of all the new possible vulnerabilities that are said to be out today and may affect the company. Audit all the systems the company is in possession of and plan accordingly. See if there are any ways to put in place a system and communications protection plan for the company. Make sure all vulnerabilities are fixed or removed from the company's environment. If there are devices that have vulnerably that can't be fixed, then they should be removed from the company's technological environment. Manage the configurations so that all unknown sources can't be downloaded on any of the company's devices, meaning turn off the unknown sources setting. Make sure the system and information integrity is strong. Create a contingency plan in case something does happen in the future. Make sure there is someone managing the security program at the company. Last but not least, avoid using any devices that have any vulnerably that can't have any controls or fixes at the least.