frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

Don't be the same, be better!

September 2019

Issue 9, Volume 9

This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel Futures!

Channel Futures MSP 501 2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

Study On Passwords Shows People Still Use Breached Passwords

Google recently released a large-scale password study that will probably give every IT manager in the country heartburn. The results of their study indicate that a disturbing percentage of users continue to use passwords after they've been warned that those passwords have been compromised.

One of the most common tactics hackers employ is called 'password spraying.' It's a simple technique. The hackers simply try several compromised passwords (even if they've been floating around the Dark Web for months) thinking that a surprising percentage will still work. Google's study confirms the hackers' beliefs to be true.

Right now on the Dark Web, there are more than 4 billion passwords known to be compromised. The scope and scale of the problem is staggering. Worse, the users who have compromised accounts are, as a rule, slow to do anything to mitigate the danger. According to the results of the study, only 26.1 percent of users who saw an alert indicating a compromised password bothered to change it. Barely one in four.

Even when users did bother to change their passwords, 60 percent of the time, the new password was found to be vulnerable to a simple guessing attack. Although in fairness, 94 percent of changed passwords wound up being stronger than the previous one.

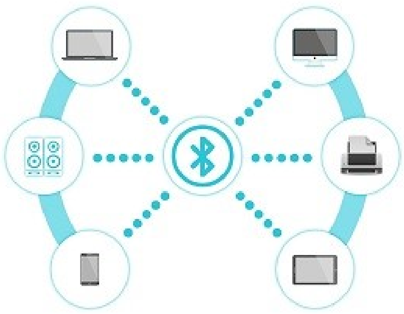
To collect the information, Google relied on a newly offered Chrome extension called Password Checkup, which it claims is superior to Firefox's Monitor and the "Have I Been Pwned" website.

The company contends that these other solutions could be exploited by hackers, summing it up as follows:

"At present, these services make a variety of tradeoffs spanning user privacy, accuracy, and the risks involved with sharing ostensibly private account details through unauthenticated public channels...For example, both Firefox and LastPass check the breach status of user names to encourage password resetting, but they lack context for whether the user's password was actually exposed for a specific site, or whether it was previously reset.

Equally problematic, other schemes implicitly trust breach-alerting services to properly handle plaintext usernames and passwords provided as part of a lookup. This makes breach alerting services a liability in the event they become compromised (or turn out to be adversarial)."

Bluetooth Security Issue Could Affect Most Devices



Recently, researchers from Boston University published a paper called "Tracking Anonymized Bluetooth Devices". The paper detailed a flaw in the ubiquitous Bluetooth communication protocol that could expose device users to tracking and even leak their IDs. As explained in the paper, many Bluetooth devices announce their presence by using their MAC addresses as the basis to generate a random number in order to prevent long-term tracking.

The team discovered a flaw in the system, and identified tokens that exist alongside MAC addresses. The researchers created what they're calling an address-carryover algorithm that is able to "exploit the asynchronous nature of payload and address changes to achieve tracking beyond the address randomization of a device. The algorithm does not require message decryption or breaking Bluetooth security in any way, as it is based entirely on public, unencrypted advertising traffic."

At the center of this flaw is Bluetooth BLE, which stands for Low Energy Specification). Introduced in 2010, it really came to the fore with the release of Bluetooth 5. The research team discovered it when they began investigating BLE advertising channels and "advertising events" within standard Bluetooth proximities.

"Most computer and smartphone operating systems do implement address randomizations by default as a means to prevent long-term passive tracking, as permanent identifiers are not broadcasted. However, we identified that devices running Windows 10, iOS or mac OS regularly transmit advertising events containing custom data structures which are used to enable certain platform-specific interaction with other devices within BLE range."

Although this technique works on any Windows, iOS, and macOS system, Android devices are completely immune. That is because the Android OS doesn't continually send out advertising messages, and instead takes the approach of scanning for advertising messages being transmitted nearby.

If all of that makes your head spin, consider this: The number of Bluetooth devices is projected to grow from 4.2 to 5.2 billion between 2019 and 2022. So this is a significant issue, deserving of attention.

New Charging Cables Could Hack Your Devices

A security researcher known as "_MG_" on Twitter has invented a modified Apple Lightning cable that could allow a hacker to remotely access any Mac computer using them. He demonstrated his new invention, dubbed the "OM.G Cable" at the Def Con hacking conference in Las Vegas recently. The Lightning Cable is used by Apple owners to charge their devices and sync data.

The OM.G cable is indistinguishable from a legitimate Lightning Cable. According to tests conducted by Motherboard, it allows a hacker to type in the IP address of the fake cable on his own device and gain access to a variety of tools on the victim's computer or phone, via a simple menu-driven system.

The cable comes with a wireless implant that allows the hack to occur. Once it's plugged into the victim's device, it creates a Wi-Fi hotspot that allows it to wirelessly transmit malicious payloads, scripts, and commands on the victim's device. Even worse, it has an impressive range of 300 feet.

In an interview with Motherboard, MG had this to say about his invention: "It looks like a legitimate cable and works just like one. Not even your computer will notice a difference - until I, as an attacker, wirelessly take control of the cable."

MG sold his home brew cables to Def Con attendees for $200 each, so there are a small number of these devices in the wild now, and the number is growing steadily. For their part, Apple has responded to the event by advising their customers to avoid buying cables from untrusted vendors and to only use the cable contained in your iPhone box.

They also explained how to spot a counterfeit cable, as follows:

"To identify counterfeit or uncertified cables and accessories, look carefully at the accessory's packaging and at the accessory itself. Certified third-party accessories have the MFi badge on their packaging. An Apple Lightning to USB cable has 'Designed by Apple in California," and either 'Assembled in China,' or 'Assembled in Vietnam' or 'Industria Brasilerira' on the cable about seven inches from the USB connector."

It's good information and something to keep a close watch on. This kind of hack is very hard to counter.

We now have an E–newsletter!

… but we might not have your email address! If you would like to receive our newsletter though email please visit us at **www.getfrogworks.com/newsletter** and sign up.

LeapPad Kids Tablet Found To Have Security Issues

Researchers at CheckMarx recently discovered some serious security flaws in the popular LeapPad Ultimate tablet.

The tablet was designed by LeapFrog to provide kids in the UK and Europe with a safe environment to access games, videos and educational apps.

The researchers had this to say about their discovery:

"The first thing we found is that some of LeapFrog's communications aren't encrypted. It's using very simple HTTP protocol, storing information in clear text and allowing an attacker to become a man-in-the-middle."

The researchers built a proof of concept app that allowed them to spoof the existing connection and force the device onto a rogue network. From there, they were able to inject malicious scripts into the rogue network and use them to access a variety of sensitive information from the system, such as the child's name, gender, birth year and birth month.

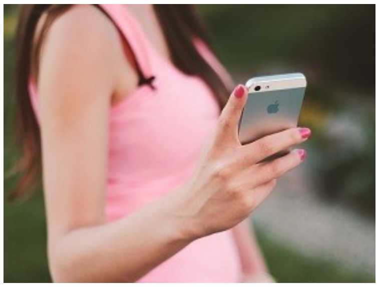
The researchers also noted that this attack methodology could allow hackers to steal information about the parents of the kids using the device, including their email addresses, phone numbers and access to payment card information.

Mari Sunderland, the VP of Digital Product Management at LeapFrog, issued a formal statement for the company, which read, in part, as follows:

"We thank CheckMarx for bringing these security issues to our attention, as the safety of the children who use our products is our top priority. When you know that the main users of your device will be children, the standards you need to put on your R&D need to be the highest: Military grade. Vendors should be very responsible and understand that privacy issues for children are much worse. All this needs to be taken into account to make sure your solution is as safe as possible."

It's a wonderful sentiment, and one hopes that LeapFrog's next solution will be more robust.

Apple Will Stop Listening To Siri Recordings For Now



Not long ago, both Google and Apple found themselves in hot water when it came to light that both companies had been making use of third-party partners to review Siri recordings.

As the companies explained at the time, their goal was to make their voice recognition software more efficient and more effective.

After they found themselves at the center of a controversy over it, Apple has announced that they have formally suspended the program worldwide while they conduct a review.

A company spokesman had this to say:

"We are committed to delivering a great Siri experience while protecting user privacy. While we conduct a thorough review, we are suspending Siri grading globally. Additionally, as part of a future software update, users will have the ability to choose to participate in grading."

In a similar vein, Google announced that it was putting its evaluation program on hold in Europe only for three months.

Johannes Casper, the Hamburg Commissioner for Data Protection and Freedom of Information, had this to say with regards to Google's current policy and a possible conflict with Europe's GDPR data-protection laws:

"The use of language-assistance systems in the EU must follow the data-protection requirements of the GDPR. In the case of the Google Assistant, there are currently significant doubts. The use of language-assistance systems must be done in a transparent way, so that an informed consent of the users is possible. In particular, this involves providing sufficient information and transparently informing those affected about the processing of voice commands, but also about the frequency and risks of mal-activation."

Kudos to the EU for making a big enough deal about this to rein Apple and Google in. Here's hoping that pro-privacy forces ultimately prevail worldwide. As good as Google Assistant and Siri are, it's important that safeguards are put in place to help preserve privacy.

Facebook Is Making Changes To Privacy Following Huge Fine

We're talking about the result of a massive five billion dollar fine over violations surrounding the Cambridge Analytica scandal. While the staggering size of the fine made all the headlines, there's more to the company's agreement than just several billion dollars.

In addition to the fine itself, the company has also accepted an agreement.

It forces Facebook to implement a new privacy framework, and to be monitored and held accountable for decisions it makes about its users' privacy and information it collects on them.

The FTC Press release reads, in part, as follows:

"The order requires Facebook to restructure its approach to privacy from the corporate board-level down and establishes strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy and that those decisions are subject to meaningful oversight (for a period of not less than twenty years)."

Facebook also published a statement about their acceptance of the fine, but it offered little in the way of new information. Digging a bit deeper, however, some of the details of the changes coming to Facebook include the following:

The formation of an independent privacy committee - The committee will be appointed by an independent nominating committee and be comprised of Facebook's board of directors. The FTC says this will help limit CEO Mark Zuckerberg's formerly unfettered control over decisions affecting user privacy.

The appointment of Compliance Officers - These people will report to the new privacy committee and will be tasked with monitoring the entire company's privacy program. The Compliance offers are not appointed by Facebook's CEO or any Facebook employee, and no Facebook employee (including the CEO) can remove those officers. One of the responsibilities of the new Compliance Team will be to submit reports to the FTC.

More and better external oversight of Facebook - The FTC's ruling strengthens the role of independent third-party assessors who will conduct independent reviews of Facebook's privacy program at two-year intervals.

Will these steps be enough? Only time will tell, but it's certainly a great start. Kudos to the FTC for holding Facebook accountable and trying to be a force for change.