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

Ribb"IT" Review

"It is only the farmer who faithfully plants seeds in the Spring, who reaps a harvest in the Autumn."

-B. C. Forbes

October 2018

Issue 10, Volume 8

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

High Frequency Audio Computer Monitors May Expose Screen Activity

It may sound like something straight out of a science fiction movie, but recently, researchers have made a disturbing discovery. Using nothing more than an off-the-shelf microphone, it's possible for an attacker to determine what content you're viewing on your computer monitor.

The researchers tested a variety of LCD screens (with both LED and CCFL backlighting) and observed that the high-pitched noise made by the monitors changed as the content displayed on the screen changed.

The research team tested a variety of methods of recording audio data from the monitors in question, and found that they could capture sufficient data with a few methods. First, a smartphone positioned near the screen, second a compromised smart virtual assistant (like Google Home or Amazon's Alexa), and third, using a parabolic microphone from up to ten meters distant.

Even more disturbing, the researchers discovered that an attacker could correctly identify the website a victim was looking at with up to 97 percent accuracy if the microphone was close to the monitor, and with 90.9 percentaccuracy with microphones placed at some distance.

Worst of all, subtle changes in the pitch of your display screen make it possible for hackers to identify what specific characters are being displayed with an accuracy that ranged from 88 percent (more distant microphones) to 98 percent (microphones in close proximity to the monitor). This makes it entirely possible to glean passwords and other sensitive information.

Granted, this is an extremely exotic form of attack that requires a great deal of advance preparation by the attacker. Because of this, it's unlikely that it will see widespread use anytime soon. Even so, it's something that a careful and determined hacker could do right now using off the shelf technology, and there's very little the victim could do to prevent it.

While we're unlikely to see equipment manufacturers take the necessary steps to mask acoustic emanations, robust on-site physical security measures would make detection of this type of attack fairly easy.

New Versions Of Ransomware Continue To Wreak Havoc

2017 was "The Year of Ransomware." It saw an incredible number of ransomware attacks and infections, paired with a tremendous number of innovations.

Although 2018 hasn't seen quite the same level of ransomware activity, it's still a major threat with one company coming under attack about every ten minutes.

Although there haven't been as many innovations so far this year, that doesn't mean they're not occurring, and some of the new ransomware strains are particularly nasty.

Of interest, this year has seen a rise in 'Cryptojacking', which is a variant of a classic ransomware attack where the malware mass encrypts files on the victim's machine while simultaneously installing cryptocurrency mining software.

This should come as no surprise given the rise in popularity of cryptocurrency, but it does add a disturbing new wrinkle to ransomware attacks. Even after you get your files back, lurking in the background there is a rogue process that's slowing your system and ultimately putting money into the bank accounts of the hackers.

Most recently, an Obama-themed cryptojacker has been making the rounds.

The ransomware itself is nothing out of the ordinary. It predictably locks your files, demands payment, and installs a Monero miner in the background.

Obama is not the first world leader to unwittingly become the face of ransomware. In 2016, Candidate Trump was featured in a malware strain that proved to be a work in progress. It would infect machines, but didn't actually encrypt files. It's unclear if a working version was ever deployed in the wild.

The Obama strain contains code fragments that indicate Chinese origin. There's circumstantial evidence that leads some security researchers to believe it may be the work of a Chinese hacker known only as "Rocke," but so far, there's no definitive proof.

As things stand now, there's no good defense against this most recent threat, save for continued vigilance.

Cortana May Have Flaw Allowing Unauthorized System Access

Researchers at McAfee have demonstrated a method that hackers could use to perform an end-run around Cortana and access data, run malicious code, or even change a locked computer's password. In this case, however, the emphasis is on the word "could."

The researchers readily admit that this attack is high risk, has never been seen in the wild, and has little possibility of going undetected for a variety of reasons. Even so, the research is disturbing and does point to a valid weakness that bears further investigation.

The setup process alone is daunting. First, the attacker would need to perform a significant amount of advance preparation. This includes going so far as to create a Wikipedia entry that could get past that site's army of talented editors and fact checkers, and then somehow inserting a link to a poisoned/compromised domain in the entry. That alone would be a challenge.

Once the Wiki page was up, with the poisoned link at the ready, the attacker would need physical access to the device in question.

Then, the user would have to have Cortana enabled from the lock screen.

Assuming that hurdle was also cleared, the attacker could begin asking Cortana questions, which would prompt her to search the web for information about the topic being inquired after.

Cortana is designed in such a way that if web-based resources are needed to answer the query, it will look for a Wiki Page and display the link found there.

If the hacker succeeded in doing all of that, Cortana would access the poisoned web page via a scaled down version of Internet Explorer 11, which would then allow the hackers to send malicious code via the now-established connection.

Is this a real threat? Absolutely. It is within the realm of possibility that a hacker could do everything described above.

Is this even remotely plausible? No. There are simply too many points of failure for this to be considered a genuine threat, as underscored by the fact that nobody has ever seen anything like this in the wild.

Hackers tend to prefer simple, elegant solutions. While it's not outright impossible to imagine a hacker giving this a go just for fun, it's hard to see this as an emerging threat, or something to be greatly concerned about.

Some Apple iPhone 8's May Have A Manufacturer Defect

Do you own an iPhone 8? If so, you may have problems. Apple has recently reported that a small percentage of iPhone 8s "contain logic boards with a manufacturing defect.

Affected devices may experience unexpected restarts, a frozen screen, or won't turn on."

The company has isolated the defect to phones manufactured between September 2017 to March 2018, in Hong Kong, India, Japan, China, New Zealand, Macau, and the United States.

To find out if you've got one of the impacted iPhone 8s, head to the company's website and use the tool they've placed there, entering your phone's serial number. If your phone is one of the defective devices, Apple will repair it free of charge for up to three years after the sale.

Note, however, that some types of damage may incur fees to repair, specifically in the instance of a cracked screen or similar.

Apple's handling of the issue has so far been quite good. They were quick to acknowledge the mistake and isolate it to a very specific frame of time, and equally quick to create a checking tool. Their repair policy is generous, as is the impressive three-year window.

It's unfortunate that the manufacturing error occurred. However, the reality is that many companies would not have been as forthcoming as Apple has been, nor as generous with their repair policy.

Kudos to Apple for their handling of the issue. If you're considering buying a new iPhone, don't let this hiccup change your mind. Although the company isn't perfect, you'll find few companies that can top Apple in terms of taking care of their customers. There's a reason their customers are more like fans, and companies of all shapes and sizes would do well to emulate Apple as best they can.

Tech Support Scammers Are Advertising Online

Tech Support scams are nothing new, but they are getting increasingly sophisticated. Worse, tech giants like Google are finding it notoriously difficult to detect them.

A report recently released by the venerable data security firm, Symantec, indicates that tech support scammers are increasingly integrating call optimization into their schemes, which allows them to insert phone numbers into web pages dynamically. Among other things, this allows the scammers to display the phone number of someone who speaks the language of the victim, which makes the whole act more convincing and much more likely to succeed.

In recent years, tech support scams have begun promoting their "services" via ads, where they claim to be legitimate, authorized service centers for companies like Apple, Microsoft, or Dell. The brand recognition and professional presentation combine to put their victims at ease.

They're so slick and professional, and their "employees" so good at mimicking the employees of legitimate service centers that it can be virtually impossible to tell the real companies from the fake ones.

David Graff, Google's Director of Global Product Policy had this to say about the matter:

"For many years, we've consulted and worked with law enforcement and government agencies to address abuse in this area. As the fraudulent activity takes place off our platform, it's increasingly difficult to separate the bad actors from the legitimate providers."

Google is taking steps to try and combat the rising threat. Recently, they've made a change to their policy as it relates to tech support companies, only accepting ads from verified third-party support vendors.

Even with this added layer of protection, however, the tech support scam is thriving. Scammers have already begun taking steps to get around the new restrictions by cold-calling their victims. For the most part, this has proved to be a successful tactic for them. However, in at least one instance, where the scammers called the New Zealand Police, it ended quite badly for the criminals.

Microsoft Outlook is Rolling Out New Design

Microsoft is making some long overdue and welcome changes to Outlook to include the Windows and the Web-based version.

People who use either one will now see a "Coming Soon" option that allows users to toggle between the version they've got now, and the new and improved version with the changes.

As to those changes, they fall broadly into three groups:

1. Better Organization - The improved Outlook offers intelligent technology, specialized icons, visual changes and a "highlights" feature that are all designed to help you manage your time better and provide a greater level of focus on your daily and weekly activities.
2. Improved Speed and Efficiency - The redesign is sleeker and faster. Using it will allow you to schedule meetings, read and act on emails and write new emails much more quickly than the old version.
3. More Customization - Hotmail users know only too well that Outlook on the web has lagged behind its competitors in terms of customization, and the redesign seeks to change that. Microsoft is playing a bit of catch up here, but any improvements on this front are welcome indeed. Among other things, you can now apply additional themes, personalize your inbox and simplify the ribbon.

There's no word yet on how long the new features will be offered as an opt-in option, but of course, at some point, the company will mandate the change.

On balance, these are good changes. Perhaps more modest than long-time users would like to have seen, but again, any changes to one of the oldest email systems still around have to be counted as a positive.

Kudos to Microsoft for keeping Outlook reasonably up to date, and here's hoping that the user base embraces them which we hope will encourage the company to make additional improvements.