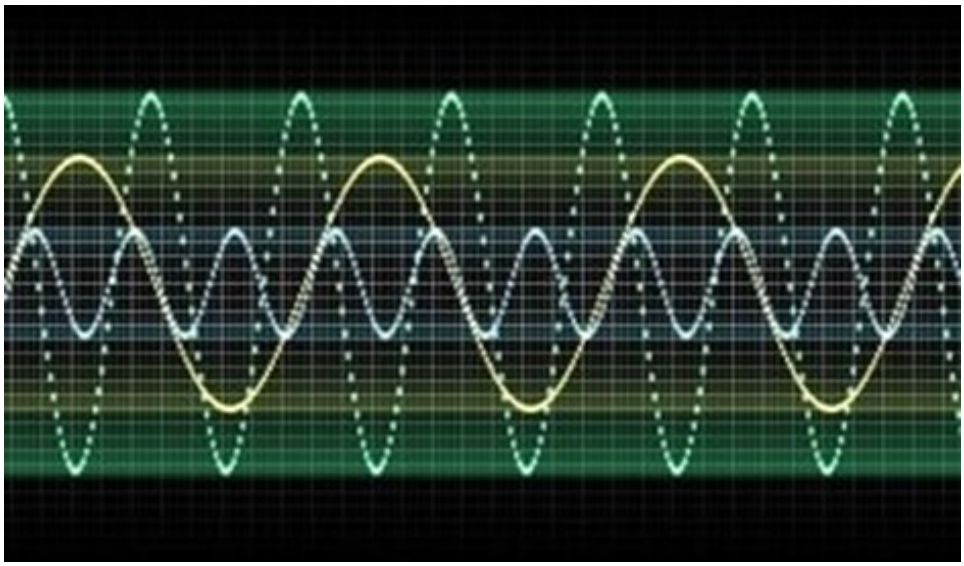
frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

While it is February one can taste the full joys of anticipation. Spring stands at the gate with her finger on the latch.



Sound Waves May Be Used In Future Hard Drive Attacks

Another week, another attack vector, and this one deserves extra points for creativity.

New research has proved the viability of using something as simple and innocuous as sound waves to disrupt the normal functioning of HDDs, which can be used to sabotage a wide range of equipment from Pcs, to CCTV systems, ATMs and more.

Researchers have toyed with, and been aware of the possibility of using sound waves to disrupt the normal functioning of an HDD for more than a decade, but the most recent research conducted by scientists from Princeton and Purdue universities have outlined exactly how such an attack could be carried out.

The attack exploits a peculiar design feature of HDDs. Because they store large amounts of data on small platters, they're designed to shut down in the presence of excessive vibration to avoid scratching or damaging the platter, and thus, destroying information on the drive.

If a hacker can determine the optimal attack frequency against a given HDD, then he could play a sound aimed at the drive that would cause it to stop functioning. If the sound were played long enough, it would require the system to be manually restarted to get it working again.

As the researchers demonstrated, finding the optimal attack frequency is a trivial enough task, but it should be noted that this is a fairly exotic type of attack, and not likely to see widespread use.

The biggest threat one would potentially face from such an

February 2018

Issue 2, Volume 8

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

*"As a business owner, you don't have time to waste on technical and operational issues. That's where we **shine**! Call us and put an end to your IT problems finally and forever!"*

- Alex Bleam, Frogworks

attack would be the disruption of the functioning of security cameras to create a blind spot at a facility, which could then be physically breached. But given that the tones are within the range of human hearing, anyone in the vicinity could come and investigate.

Nonetheless, it's an intriguing bit of research with potentially damaging implications.

Virus Spread Through Facebook Messenger Mines For Cryptocurrency

Facebook scams are fairly common occurrences, owing to the sheer size of the platform's user base. It's no surprise that there's a new one making the rounds that you should be aware of.

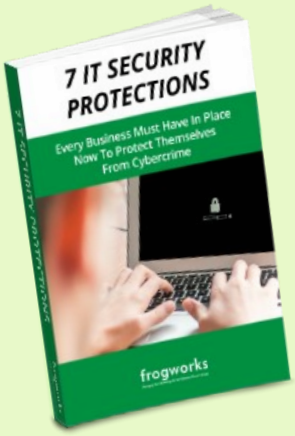
This latest threat was discovered by researchers at Trend Micro, and makes use of Facebook Messenger. If you get a message containing an embedded video file saved as a zip (the file name usually appears as "video_xxxx.zip"), don't click on it, even if it's from someone you know.

This file is a modified form of a legitimate piece of software called "XMRig", an open source project that allows users to mine the cryptocurrency called Monero.

When the user clicks on this poisoned version, it will direct them to a website controlled by the hackers, in addition to quietly installing the corrupted software in the background. Once installed, the hackers put the infected PC's processor to work for them, creating a distributed network of hash power to solve advanced cryptographic puzzles and generate new Monero "coins" for themselves.

The hackers have gone to some lengths to mask their true intentions. The site appears to be a video streaming service, and users who click on the embedded file will actually see a video playing. Of course, the website is also part of the C&C structure.

Have you ever lost an hour of work on your computer?



After working with dozens of small and mid-size businesses in the DC Metro area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs on average.

Gain Instant Access To Our Free Report, "7 IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime" TODAY! at https://www.getfrogworks.com/Cybercrime

Or call us today at (240) 880-1944

There are several intriguing things to note about this new threat:

- It only affects people who use the Google Chrome web browser
- It only affects PCs and Laptops. Smartphones are not impacted in any way
- The miner software is actually controlled via the C&C server, meaning that the hackers can upgrade their malware, adding new functionality in the blink of an eye

So far, the virus has been spreading mostly in south east Asia, but has also begun appearing in the Ukraine and Venezuela. Given the global nature of Facebook's user base, this is wholly unsurprising, so be on the lookout for it. Don't click embedded files in Messenger, even if you think you know the sender.

Weird Sounds Coming From Your Speakers? Could Be A Hacker

Have you been hearing strange, otherworldly sounds on your Bose or Sonos speakers? If so, rest assured that your speakers aren't haunted. They've likely been hijacked by hackers.

Researchers at Trend Micro have confirmed that some models (the Sonos Play:1, the Sonos One and the Bose SoundTouch) of both brands of speakers are vulnerable to hacking if the speaker is connected to a misconfigured network.

If the hackers find such a speaker, they can take control of the speaker and direct to play any audio file hosted at a specific URL.

It should be noted that this is an extremely exotic, fairly elaborate hack, and one that's not likely to gain the hacker much, if anything in the way of useful information about the target network. Overwhelmingly, if and where this hack is seen at all, it will be used to play pranks on the target. About the worst thing that could happen is that the hacker would play a particularly annoying or alarming sound (a woman screaming, glass breaking, a baby crying or similar), which might lead to some sleepless nights or confusion, but not much else.

Better Parental Controls Underway For Apple Devices

Recently, a group of investors wrote an open letter to Apple, urging the company to do more in regards to offering better and more robust parental controls on the devices the company makes. Although the group of investors control some $2 billion in Apple stock, this is a drop in the proverbial bucket, given the company's $900 billion market cap. Nonetheless, the letter seems to have gotten Apple's attention.

In a statement published in the Wall Street Journal, the company said: "We think deeply about how our products are used and the impact they have on users and the people around them. We take this responsibility very seriously, and we are committed to meeting and exceeding our customers' expectations, especially when it comes to protecting kids."

Previously, the company has touted the suite of parental controls it's had in place on the devices it makes since 2008. For example, every iPhone sold has a settings app with a parental controls section that allows adults to control in-app purchases, install and delete apps, and restrict website access.

Those are all good things, but the group of investors is pushing for more. Although the company has not released any details about their planned enhancements, it does appear that the letter has prompted them to think even more deeply about the matter, and in that same letter, also requested that apple aid research that studies what impacts excessive smartphone use has on mental health.

To their credit, Apple has done more with parental controls than many, if not most other tech companies, and it is very good to see that they're listening and responding to the concerns of their investors. This kind of responsiveness bodes well, and depending on the particulars of their plan, it could well cause other companies in the industry to attempt to match their moves.

Even so, it's worth making note of, because if a hacker is able to take control of a speaker connected to your network, it means that there's a misconfiguration somewhere that could lead to a more serious hack down the road. If it happens to you, it's well worth reviewing your network setup and security settings.

A spokesman for Sonos had this to say about the hack: "...looking into this more, but what you are referencing is a misconfiguration of a user's network that impacts a very small number of customers that may have exposed their device to a public network. We do not recommend this type of set-up for our customers."

Interestingly, this isn't the first time such a hack has been seen. In 2014, a developer created a hack that went by the name "Ghosty" that did more or less the same thing.

Select HP Laptop Models Recalled Over Battery Issue

Did you purchase an HP laptop between December of 2015 and December of 2017? If so, then you may have problems.

The US Consumer Product Safety Commission has been made aware of eight instances where HP battery packs overheated, charred, or melted, creating a worrisome fire hazard that has gotten the attention of user groups scattered all over the internet.

It also got the attention of HP itself, and the company recently announced "a worldwide voluntary safety recall and replacement program" for laptops shipped during the timeframe mentioned above.

If you own one of the following models, you may be impacted:

HP ProBook 640 G2
HP ProBook 645 G2
HP ProBook 650 G2
HP ProBook 655 G2
HP ProBook 640 G3
HP ProBook 645 G3
HP ProBook 650 G3
HP ProBook 655 G3

HP ZBook 17 G3
HP ZBook Studio G3
HP ZBook 17 G4
HP x360 310 G2
HP Pavillion x360
HP ENVY m6
Or the HP 11 Notebook PC

You can visit HP's website and download a tool you can use to test your laptop to see if it has one of the defective battery packs. A BIOS update is also available that will safely and completely discharge the battery. Although of course, until you get a replacement, you'll only be able to power your laptop via the AC power supply.

According to the company, "Many of these batteries are internal to the system, which means they are not customer replaceable. HP is providing battery replacement services by an authorized technician at no cost."

While it's a nice gesture, it would be even better if the company hadn't shipped the defective batteries in the first place and caused a major inconvenience to its customers. This most recent recall comes on the heels of another one less than a year ago, in which the company recalled more than 100,000 similarly defective laptops at the end of January, 2017.