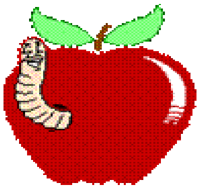
News from



The GLORIOUS SOCIETY OF THE WORMHOLE

June 2018

Hello Worms

Hi Worms,

June is Field Day month. I encourage all to at least attend if not participate in one of the many Field Day operations around the Tampa Bay area. Many of the Pinellas clubs are combining operations. While the Wormhole has not formally declared to be represented (yet) I am sure many of our members will be in attendance. And if anyone not a member of any of the other clubs then declare yourself the Wormhole representative.

I just noticed how long the list of yearly folders in my Wormhole Newsletter folder is getting. My first year is 2005 with the first newsletter dated February of that year. That makes 209 newsletters I have put out in 13 years. The format has changed of late to accommodate those who read it on their phone. In that time I have maybe five articles submitted by other hams, not including the national blogs that I have permission to plagiarize. I have written very few myself. You are all welcome, nay encouraged to submit an article you have written on any subject of interest to a bunch of Worms.

Talk-in is on the Wormhole repeater system. For those coming to the meeting who cannot hit the repeater we will also monitor the Honeywell club repeater on 443.050 +141.3. Bring a folding chair if you have one.

* GOOGLE CHANGING ADVERTISING *

INFOPACKETS by John Lister on May, 8 2018

Google is to tighten up its rules on election-related advertising. It will restrict who's allowed to place such an ad and give the public more detail on who's behind elections ads.

The new rules will cover election ads purchased on Google in the US. It doesn't yet appear the rules will affect ads that simply address political issues rather than specific candidates and campaigns.

One rule is that anyone placing an election ad will need to prove they are either a US citizen or a lawful permanent resident. While this becomes law, Google says it will tighten its enforcement by requiring proof that includes government-issued IDs.

All election ads will also need to include "a clear disclosure of who is paying for it." Of course, that only covers who actually pays the money to Google and won't necessarily reveal the original source of the cash. Later this year Google plans to release a special report detailing which people and organizations are placing election ads and the total amount they have spent. (Source: blog.google)

Google is also developing a searchable library of election ads that will let people find all ads placed on the site (and who placed them). That's key, as normally web users will only see ads specifically targeted at them. The library might reveal cases where campaigns are providing contradictory messages to different segments of the electorate - something that's perfectly legal, but politically questionable.

The measures are similar to that which Facebook is taking to reduce the risks of its advertising platforms being misused and abused during electoral campaigns. (Source: theverge.com)

As part of it's election-related work, Google is also trying to reduce the risk of phishing and other security attacks relating to the electoral process. It's offering campaign staff, journalists and elections officials specialized training in avoiding such attacks, along with enhanced security tools for their accounts.

IMPROVE YOU STATION AUDIO QUALITY –PART 3

The last article dealt with improving the audio amplification of your receiver. There are other controls on most receivers that help with noise.

Tune the receiver to a place where you only have atmospheric noise. Granted, for some this may not be possible due to man made noise makers. However, this will do also.

If you have a manual notch filter, try notching the noise. It may be enough to help. At the same time it could muffle the audio of what you are listening to. Possibly a compromise in adjustment may help.

Some receivers have a selection of Pass Band filters. Try each one and see how it reacts with the noise. Due to the sharper bandwidth it can make the noise seem more predominant. However don't give up here.

If you have an IF shift or Pass Band Tuning (PSB), you can try changing the pass band to reduce the noise. Try it with the various filters your receiver may have.

Receivers for a long time have an Audio Frequency (AF) gain and a Radio Frequency (RF) gain.

The AF gain is straight forward, it makes the audio louder or softer. However the RF gain is a little different.

As you turn the RF gain down, you will see the S meter reading go up. Why? The RF gain is interconnected to the Automatic Gain Control (AGC). Bringing the gain down will start making the noise floor subside. Actually it is like putting a bit of squelch on to the receiver. If the signal you are listening to is able to be heard this way, it can be much clearer. You can up the AF gain to increase volume to a comfortable level.

Your receiver has an Automatic Gain Control selection. It can be Off, fast or slow. It may just give you a numbered selection. The slower functions will allow the incoming signal you are listening to partially squelch the receiver. Sort of like decreasing the RF gain with the voice peaks. This will also make reception with less noise to hear.

These are some of thing you can experiment with to get to know your receiver better. You may be surprised on how much better you can pick out stations when you get to know your receiver better. There is more, another time.

73,

Ralph WD0EJA
BILAL COMPANY
wd0eja@isotronantennas.com

* AMATEUR RADIO PARITY ACT IN NATIONAL DEFENSE AUTHORIZATION ACT *

FEMA Disaster Emergency Communications (DEC) Division newsletter May 11, 2018
ARRL is praising the work of US Representatives Joe Courtney (D-CT), Vicky Hartzler (R-MO), and Mike Rogers (R-AL) for their successful efforts in securing language in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 that aids in the survival and growth of Amateur Radio by giving radio amateurs the right to install an outdoor antenna at their residences with the approval of their homeowners associations. This language — text from the proposed Amateur Radio Parity Act (HR 555) — formed the basis for the Courtney-Hartzler-Rogers Amendment to the NDAA. http://www.arrl.org/news/amateur-radio-parity-act-language-inserted-in-national-defense-authorization

* EXAMS PLAGUED BY CHEATER WRISTWATCHES*

INFOPACKET by John Lister on May, 17 2018 at 01:05PM

British students have been banned from wearing any form of wristwatch in exams. It follows concerns that 'smart watches' containing helpful information could be disguised as ordinary watches.

The new rules will affect most national exams for school students aged 16 and 18, including those which determined whether students can get a particular place on a university course. The rules say normally students must take off their watch and leave it in a visible place on their desk, though in some cases supervisors are collecting the watches and keeping them outside.

The changes follow on from existing rules that ban any form of smart watch that can store data digitally, including answers to exam questions. Rules banning smart watches proved inadequate when officials became aware of a range of 'cheating watches' advertised on sites such as Amazon. Unlike some more mainstream smart watches, these don't connect to cell phones, which are also banned under existing rules. (Source: bbc.co.uk)

One variant involves the watch having a digital display that replicates either an analog watch face or a digital clock. However, the watch is actually a small computer, and pressing a button replaces the display with text that the student has previously loaded onto the device. An "emergency button" will immediately switch the display back to a clock as well as disabling the other buttons in case a supervisor examines the watch. (Source: telegraph.co.uk))

Another variant of the cheating watch is an analog device, which comes bundled with a tiny Bluetooth earpiece. The watch has data storage similar to a USB flash drive and can house audio files such that pressing a watch button will read out stored text via the earpiece.

Nostalgic cheaters will be pleased to know that not all of the rule breaking involved digital watches. In some cases, students were also using what appeared to be an ordinary analog watch that in fact had a lift-up face that revealed a hiding place for a paper note.

The idea of forcing students to place the watch on the desk is to allow them to check the time if necessary but in a way that means they have no reason to touch the watch during an exam.

I decided to see what these items looked like on eBay and was surprised that there are also glasses and pens with nano ear receivers that can relay audio for the purpose of cheating on exams. The rules need to be extended to give out "certified" pens and pencils during an exam. The cheating eye glasses would certainly be harder to detect, though perhaps prescription eye glasses could be pre-registered with a photo before exams take place.

* HACKERS INFECT 500,000 ROUTERS WITH MALWARE*

arsTECHNICA Dan Goodin - 5/23/2018

Hackers possibly working for an advanced nation have infected more than 500,000 home and small-office routers around the world with malware that can be used to collect communications, launch attacks on others, and permanently destroy the devices with a single command, researchers at Cisco warned Wednesday.

VPNFilter—as the modular, multi-stage malware has been dubbed—works on consumer-grade routers made by Linksys, MikroTik, Netgear, TP-Link, and on network-attached storage devices from QNAP, Cisco researchers said in an advisory. It's one of the few pieces of Internet-of-things malware that can survive a reboot. Infections in at least 54 countries have been slowly building since at least 2016, and Cisco researchers have been monitoring them for several months. The attacks drastically ramped up during the past three weeks, including two major assaults on devices located in Ukraine. The spike, combined with the advanced capabilities of the malware, prompted Cisco to release Wednesday's report before the research is completed.

Update: FBI agents have seized a key server used in the attack. The agents said Russian-government hackers used ToKnowAll.com as a backup method to deliver a second stage of malware to already-infected routers.

"We assess with high confidence that this malware is used to create an expansive, hard-to-attribute infrastructure that can be used to serve multiple operational needs of the threat actor," Cisco researcher William Largent wrote. "Since the affected devices are legitimately owned by businesses or individuals, malicious activity conducted from infected devices could be mistakenly attributed to those who were actually victims of the actor. The capabilities built into the various stages and plugins of the malware are extremely versatile and would enable the actor to take advantage of devices in multiple ways."

Sniffers included with VPNFilter collect login credentials and possibly supervisory control and data acquisition traffic. The malware also makes it possible for the attackers to obfuscate themselves by using the devices as nondescript points for connecting to final targets. The researchers also said they uncovered evidence that at least some of the malware includes a command to permanently disable the device, a capability that would allow the attackers to disable Internet access for hundreds of thousands of people worldwide or in a focused region, depending on a particular objective.

“In most cases, this action is unrecoverable by most victims, requiring technical capabilities, know-how, or tools that no consumer should be expected to have,” Cisco’s report stated. “We are deeply concerned about this capability, and it is one of the driving reasons we have been quietly researching this threat over the past few months.”

Russian hackers mass-exploit routers in homes, govs, and infrastructure

Cisco’s report comes five weeks after the US Department of Homeland Security, FBI, and the UK’s National Cyber Security Center jointly warned that hackers working on behalf of the Russian government are compromising large numbers of routers, switches, and other network devices belonging to governments, businesses, and critical-infrastructure providers. Cisco’s report doesn’t explicitly name Russia, but it does say that VPNFilter contains a broken function involving the RC4 encryption cipher that’s identical to one found in malware known as BlackEnergy. BlackEnergy has been used in a variety of attacks tied to the Russian government, including one in December 2016 that caused a power outage in Ukraine.

BlackEnergy, however, is believed to have been repurposed by other attack groups, so on its own, the code overlap isn’t proof VPNFilter was developed by the Russian government. Wednesday’s report provided no further attribution to the attackers other than to say they used the IP address 46.151.209.33 and the domains toknowall[.]com and api.ipify[.]org.

There’s little doubt that whoever developed VPNFilter is an advanced group. Stage 1 infects devices running Busybox- and Linux-based firmware and is compiled for several CPU architectures. The primary purpose is to locate an attacker-controlled server on the Internet to receive a more fully featured second stage. Stage 1 locates the server by downloading an image from Photobucket.com and extracting an IP address from six integer values used for GPS latitude and longitude stored in the EXIF field. In the event the Photobucket download fails, stage 1 will try to download the image from toknowall[.]com.

If that fails, stage 1 opens a "listener" that waits for a specific trigger packet from the attackers. The listener checks its public IP from api.ipify[.]org and stores it for later use. This is the stage that persists even after the infected device is restarted.

Cisco researchers described stage 2 as a "workhorse intelligence-collection platform" that performs file collection, command execution, data exfiltration, and device management. Some versions of stage 2 also possess a self-destruct capability that works by overwriting a critical portion of the device firmware and then rebooting, a process that renders the device unusable. Cisco researchers believe that, even without the built-in kill command, the attackers can use stage 2 to manually destroy devices.

Stage 3 contains at least two plugin modules. One is a packet sniffer for collecting traffic that passes through the device. Intercepted traffic includes website credentials and Modbus SCADA protocols. A second module allows stage 2 to communicate over the Tor privacy service. Wednesday's report said Cisco researchers believe stage 3 contains other plugins that have yet to be discovered.

Wednesday's report is concerning because routers and NAS devices typically receive no antivirus or firewall protection and are directly connected to the Internet. While the researchers still don't know precisely how the devices are getting infected, almost all of those targeted have known public exploits or default credentials that make compromise straightforward. Antivirus provider Symantec issued its own advisory Wednesday that identified the targeted devices as:

- Linksys E1200
- Linksys E2500
- Linksys WRVS4400N
- Mikrotik RouterOS for Cloud Core Routers: Versions 1016, 1036, and 1072
- Netgear DGN2200
- Netgear R6400

- Netgear R7000
- Netgear R8000
- Netgear WNR1000
- Netgear WNR2000
- QNAP TS251
- QNAP TS439 Pro
- Other QNAP NAS devices running QTS software
- TP-Link R600VPN

Both Cisco and Symantec are advising users of any of these devices to do a factory reset, a process that typically involves holding down a button in the back for five to 10 seconds. Unfortunately, these resets wipe all configuration settings stored in the device, so users will have to reenter the settings once the device restarts. At a minimum, Symantec said, users of these devices should reboot their devices. That will stop stages 2 and 3 from running, at least until stage 1 manages to reinstall them.

Users should also change all default passwords, be sure their devices are running the latest firmware, and, whenever possible, disable remote administration. (Netgear officials in the past few hours started advising users of "some" router models to turn off remote management. TP-Link officials, meanwhile, said they are investigating the Cisco findings.

There's no easy way to determine if a router has been infected. It's not yet clear if running the latest firmware and changing default passwords prevents infections in all cases. Cisco and Symantec said the attackers are exploiting known vulnerabilities, but given the general quality of IoT firmware, it may be possible the attackers are also exploiting zeroday flaws, which by definition device manufacturers have yet to fix.

What this means is that out of an abundance of caution, users of the devices listed above should do a factory reset as soon as possible, or at a minimum, they should reboot. People should then check with the manufacturer for advice. For more advanced users, the Cisco report provides detailed indictors of compromise and firewall rules that can detect exploits.

Cisco researchers urged both consumers and businesses to take the threat of VPNFilter seriously.

“While the threat to IoT devices is nothing new, the fact that these devices are being used by advanced nation-state actors to conduct cyber operations, which could potentially result in the destruction of the device, has greatly increased the urgency of dealing with this issue,” they wrote. “We call on the entire security community to join us in aggressively countering this threat.”

CLUB MEETING

The next club meeting is June 2nd. We meet on the first Saturday every month at 11:00 Saturday morning at the Minnreg Building located at 6340 126th Ave N, Largo. Members are welcome to come in the rear area through the gate on the southeast corner of the property. Talk-in is on the Wormhole repeater system. For those coming to the meeting who cannot hit the repeater we will be monitoring the Honeywell club repeater on 443.050 +141.3. We will keep an eye peeled for you. We will take advantage of the cooking facilities with an after-the-meeting Social and Wormdog picnic.

CLUB NETS

Check in on the club net Thursdays at 1930. 442.625 + with a 146.2 tone or the 2M side at 146.850 – also with a tone of 146.2. We are always looking for volunteers to be the net control operator. Anyone interested, talk to one your club officers.

LOCAL NETS

MONDAY

1730 147.030 + Receiver sites and tone info http://www.qsl.net/wd4scd/ St Pete Yacht Club ARC

1830 147.060+ no tone St Pete ARC daily net St Petersburg

1900 144.210 USB CARS, vertical polarization Clearwater

1900 147.135 +146.2 Zephyrhills ARC Zephyrhills

2000 147.165+ 136.5 Brandon ARS from Brandon

2000 50.135 Pinellas ARK Pinellas County

2030 NI4CE system EAGLE Net, NTS traffic net, NI4CE system

2030 145.450 Pinellas ARK Pinellas County

TUESDAY

1830 147.060 no tone   St Pete ARC daily net   from St Petersburg

1900 50.200 USB   6M net   Brandon ARS

1900 28.450   WCF section net   Clearwater

1900 NI4CE system   WCF Section VHF ARES   NI4CE system

1930 145.170 & 442.4 both pl 156.7 Pinellas ACS net   Clearwater

1930 444.900 +141.3   Sheriff's Tactical ARC   Tampa

2000 NI4CE system   WCF Skywarn net   NI4CE system

2000 147.105+ 146.2   Tampa ARC net   from Tampa

2000 28.365 USB   simplex   Brandon ARS

2030 NI4CE system   EAGLE Net, NTS traffic net   NI4CE system

2100 28.465 USB   10/10 net   from Orlando

WEDNESDAY

1930 146.30   Hillsborough ARES/RACES simplex net from Tampa

1830 147.060 no tone   St Pete ARC daily net   from St Petersburg

1930 52.020 simplex   Suncoast 6'ers   from St Petersburg

1930	NI4CE system	WCF Section Digital Info Ne	NI4CE system
2000	147.105 146.2	Greater Tampa CERT net	from Tampa
2000	146.97- 146.2	Clearwater ARS	from Clearwater
2030	NI4CE system	EAGLE Net, NTS traffic net	NI4CE system
2100	NI4CE system	Tampa Bay Traders Net	non-affiliated

THURSDAY

1800	146.52 simplex	Hillsborough ARES/RACES	North Tampa
1830	147.060 no tone	St Pete ARC daily net	from St Petersburg
1900	444.750 +146.2	Fusion net	from Tampa
1930	146.850- & 442.625+ both pl 146.2	Wormhole	from St Petersburg
1930	146.6385 -127.3	Lakeland ARC	from Lakeland
1915	224.660- no tone	St Pete ARC	from St Petersburg
2030	NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

FRIDAY

1830 147.060 no tone St Pete ARC daily net from St
Petersburg

2030 NI4CE system EAGLE Net, NTS traffic net NI4CE
system

SATURDAY

0730 3.940 (7.281 Alt.)+/- QRM WCF Section HF Net from
WCF

1830 147.060 no tone St Pete ARC daily net from St
Petersburg

2030 NI4CE system EAGLE Net, NTS traffic net NI4CE
system

SUNDAY

0800 3.933 Florida Traders Net non-affiliated

1830 147.060 no tone St Pete ARC daily net from St
Petersburg

1930 NI4CE system WCF Section Net NI4CE
system

2000 147.550 simplex 550 Simplex Net
Pinellas County

2030 NI4CE system EAGLE Net, NTS traffic net NI4CE
system

2100 144.210 USB Clearwater ARS vertical
orientation

FOR SALE / WANTED

Anyone having something for sale or who might be looking for an item let me know. I will not print phone numbers or email addresses unless specifically told to since this newsletter might end up on the web. The exception is when I get the information off the web. If you are a member of the Wormhole then you have all the information you need on a club roster and if you are not a member .. why not? OK, if you are not a member you can contact me at the email address at the end of this newsletter, I will give you the information to contact the person involved.

FOR SALE, For sale: New MFJ TNC 1270X, never used in original box with manual and cables. $30. Dean Sever W8IM

FOR SALE, Mosley TA-33M 10-15-20M beam with the 40M add on kit. Antenna is on the ground and in good shape. There are several parts that need replacement. The 40M kit is new in box. Antenna is broken down into six or seven feet sections so easy to handle. Asking $400, talk to me, Bill AG4QX at arrl dot net or see me at the meeting.

FOR SALE, Cushcraft A4S 10-15-20M beam, on the ground. There are several parts that need replacement. Asking $300, talk to me, Bill AG4QX at arrl dot net or see me at the meeting.

FOR SALE, 13 element, 14.5 ft 220 beam. Wormhole property, $20, contact Bill AG4QX or any other officer. **Free to any Wormhole member or other club.** Pickup at Bill's house.

HAMFESTS

August 18 **TARCFest**, TARC Clubhouse, 22nd St at the river, $4 entry plus $3 to tailgate, inside tables $15 in advance, talkin on 147.105 +146.2, more info at http://hamclub.org/

November 3 **LARC Hamfest**, Lakeland, Revolution Church of Lakeland, 7315 Kathleen Road, Talk-In on 146.685 tone 127.3, For info contact Kevin Rought , N4KWR 863-393-4336 http://lakelandarc.org

November 10 **SPARCFest**, Pinellas Park, SPARCFest, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, Southeast corner of US 19 and 49th Street, Talk-in on 147.060+ no tone. VE testing at 0900. For more information go to http://www.sparc-club.org/sparcfest.html

December 7 & 8 **Plant City, the 2018 Tampa Bay Hamfest is the West Central Florida Section Convention, Friday and Saturday, at the Expo Building in the Strawberry Festival grounds, advanced admission $9, at the door $10, for information contact Bill Williams AG4QX,** chairman@fgcarc.org **or go to** http://www.tampabayhamfest.org **or you can just ask me, Jim or Dee at a meeting ;-)**

Mid January	Frogman swim in Tampa Bay. http://www.tampabayfrogman.com/
Last full weekend January	Winter Field Day, http://www.spar-hams.org/index.php
Late January	Gasparilla celebration
Late February	West Central Florida Tech Conference http://arrlwcf.org/wcf-special-events/wcftechconference/
March/April	MS Walks
March/April	Mass Casualty Exercises
Late April	Southeastern VHF Society Conference, http://www.svhfs.org
Late April	March For Babies (was March of Dimes) https://www.marchforbabies.org/Registration/Events
Late April	Florida QSO Party
Early to Mid May	BikeMS Citrus Tour bike ride http://www.citrustour.org/register.php
Mid-May	Annual Armed Forces Crossband Test
Mid-May	Florida Hurricane Exercise

Late May	Wormfest
Early June	Museum Ships on the Air
Fourth weekend in June	Field Day http://www.arrl.org/contests/announcements/fd/
July 3/4	Midnight Run in Largo http://www.kiwanismidnightrun.com/
August	International Lighthouse/Lightship Week https://illw.net/
October, 3rd weekend	JOTA, Scout Jamboree-on-the-AIR (around 14.280MHz)
Early December	ALS bike ride in Walsingham Park
December, first full weekend	Ride & Run With The Stars in Fort DeSoto Park
December, second weekend	Tampa Bay Hamfest http://www.fgcarc.org/

YOUR WORMHOLE OFFICERS

Bill AG4QX is President and editor of this newsletter, Treasurer is Jim KD4MZL, Paul KA4IOX is the Secretary, Dee N4GD is the Repeater Trustee and Mike K4ZPE is both our club Vice President and webmaster.

YOUR WORMHOLE REPEATERS

442.625 + PL 146.2

146.850 - PL 146.2

The Wormhole repeaters are both now dual mode Yaesu DR-1X. FM analog as always and now Yaesu Fusion, a C4FM/FM digital mode. The repeater crew updated the software on May 3, 2016.

The Wormhole website is at: http://www.TheWormholeSociety.org.

West Central Florida Section website: http://www.arrlwcf.org/.

The ARRL website is at: http://www.arrl.org/

This newsletter is written for The Glorious Society of the Wormhole, an ARRL affiliated amateur radio club located around the Seminole section of Pinellas County Florida. Anyone wishing to be added or removed from The Glorious Society of the Wormhole mailings please write to me at the address below and thy will be done.

73,
Bill Williams
AG4QX
ag4qx AT arrl DOT net