News from

The GLORIOUS SOCIETY OF THE WORMHOLE

March 2024

Hello Worms

YES, I forgot to send this newsletter early in the week. SORRY.

I think we all survived Orlando Hamcation one more time. I was at the back of the tailgate area selling until Sunday morning when I went inside, outside was dead Saturday afternoon. There were plenty of shoppers but I guess they all got tired Saturday afternoon and went somewhere for adult beverages.

Bill N1CDO found a new product that will make antenna tuning much easier. I just need to figure out how to spray the dipole at 35 feet.

Before the meeting the radio will be on for information about and directions to the meeting but that will discontinue when the meeting starts. We will continue with Zoom for now but the 40 minute limit does make it awkward at times. The Zoom information is the same as all the other meetings and is listed towards the end of this newsletter.

In the meeting we will have donuts, water and soft drinks (probably only root beer). Bring your drink and lunch if you want. We will not be cooking but we have access to the Chamber of Commerce kitchen which has a microwave and a toaster oven so you can heat up/cook what you bring.

* RESEARCHERS DEMONSTRATE LIQUID METAL RAM*

tom's HARDWARE By Christopher Harper published January 22, 2024

Researchers demonstrate liquid metal RAM, bringing us closer to flexible, implantable hardware – and to our Terminator 2 nightmares.

FlexRAM is currently limited in speed and durability, but breakthrough bodes well for the future of flexible tech. This liquid metal RAM stems from research done by researchers at Tsinghua University in China. As reported by IEEE Spectrum, FlexRAM is the first fully flexible resistive RAM device. Its main components involve droplets of liquid metal gallium (charge used for 1/0 binary memory values) suspended and injected into Ecoflex, which is a stretchable biopolymer.

According to Jing Liu, one of the researchers at Tsinghua who worked on FlexRAM, this offers "a theoretical foundation and technical path for future soft intelligent robots, brain-machine interface systems, and wearable/implantable electronic devices." While this is a revolutionary achievement and may indeed put us closer to a sci-fi future, it's important to contrast this with the actual performance of FlexRAM today.

The current version of FlexRAM is comprised of eight FlexRAM storage units, which can manage one byte of data information. Phrasing in the original publication could mean this is one byte per unit (which sounds about right), or one byte for the entire array. In either case, that's hardly consumer-grade memory capacity. And currently, the tech is only good for 3,500 cycles, rather than the millions that some more traditional (and very non-flexible) memory is capable of.

* CANNED AIR ACHIEVES SUPERSONIC SPEEDS*

tom'sHARDWARE by Mark Tyson

It is no surprise these PC air duster cans are so effective.

Ed Note: The article has a few pictures but the video is good and shows it all. Link at the end.

Ordinary canned air products shoot out jets of gas with a surprising amount of vigor. A precision engineering and machining YouTuber, Cylo's Garage, noticed telltale 'shock diamonds' in the stream emitted by his Staples-branded canned air and felt compelled to investigate further. Using a Schlieren imaging setup, the YouTuber managed to confirm that the humble air duster was pushing out a supersonic flow of gas (h/t Hackaday).

Like many a fascinating discovery, Cylo's Garage first noticed the supersonic jets emitted from the canned air nozzle by accident. Checking the air jet with a bright light in the background, confirmed that the Staples Electronics Duster was operational, but upon pulling the trigger fully the YouTuber noticed what looked like shock diamonds...

For some background, Cylo's Garage explained that shock diamonds are a type of air pattern commonly visible in the trail of a supersonic jet or rocket. Overlapping shock and expansion waves interfere with one another to create the characteristic diamond shapes in the air. These are easy to see behind a jet or rocket, propelled by fuel combustion, with the light and dark areas in the wake of the engine representing waves of contrasting air density. However, this phenomenon seemed improbable coming from a jet of ordinary canned air with perhaps 70 PSI.

About halfway through the video from Cylo's Garage, we get to see how supersonic air speeds were confirmed using a rudimentary Schlieren imaging setup. All that was needed was a simple lens, a razor blade, an imaging sensor, and a light source. See this test setup, above. This admittedly "janky" set up more or less confirmed shock diamonds in the flow of gas from the can.

Pleased with the first quick experiment, Cylo's Garage decided to refine the test method and apparatus. At six minutes in, we see a new set of test equipment put together with a far better lens and a columnated light source. From seven and a half minutes you can see the first air jets recorded using the new apparatus.

In tests, the canned air soon ran out of pressure between bursts, but more consistent shock diamonds were pictured from the nozzle of an air compressor (90 PSI). However, the YouTuber's favorite demo was delivered using the ball pump nozzle on the air compressor hose. Have a look through the gallery above for some of the great shock diamonds emitted from the canned air and various nozzles attached to a shop compressor.

https://www.tomshardware.com/desktops/pc-building/an-ordinary-squirt-of-canned-air-achieves-supersonic-speeds-engineer-spots-telltale-shock-diamonds?lrh=7f66708411428c65732192f0bd182309a79adecf791281e47053ac8335ba904a

* 3 MILLION SMART TOOTHBRUSHES HACKED*

ZDNET by Steven Vaughan-Nichols, Senior Contributing Editor

What's next, malware-infected dental floss? But seriously: It's a reminder that even the smallest smart home devices can be a threat. Here's how to protect yourself.

It sounds more like science fiction than reality, but Swiss newspaper Aargauer Zeitung reported that approximately three million smart toothbrushes were hijacked by hackers to launch a Distributed Denial of Service (DDoS) attack. These innocuous bathroom gadgets -- transformed into soldiers in a botnet army -- allegedly knocked out a Swiss company for several hours, costing millions of euros in damages.

Or, did they? Sources, such as Bleeping Computer and Bleeping Media, found it hard to credit this toothsome tale. And now the security company Fortinet, which helped give the original story credence, is admitting that mistakes were made.

In a note to ZDNET, a Fortinet representative said, "To clarify, the topic of toothbrushes being used for DDoS attacks was presented during an interview as an illustration of a given type of attack, and it is not based on research from Fortinet or FortiGuard Labs. It appears ... the narrative on this topic has been stretched to the point where hypothetical and actual scenarios are blurred."

The story had claimed that the compromised toothbrushes were running Java, a popular language for Internet of Things (IoT) devices. Once infected, a global network of malicious toothbrushes supposedly launched their successful attack.

The repurposed toothbrushes supposedly accomplished this by flooding the Swiss website with bogus traffic, effectively knocking services offline and causing widespread disruption.

Although this story wasn't real, the episode underlines the ever-expanding threat landscape as the IoT becomes increasingly embedded in our daily lives. "Smart" toothbrushes are now 10 years old. Devices that once seemed harmless and disconnected from the digital ecosystem are now potential entry points for cybercriminals. The implications are vast, not only for individual privacy and security but also for national infrastructure and economic stability.

As Stefan Zuger, director of system engineering in Fortinet's Swiss office, said, "Every device that is connected to the Internet is a potential target – or can be misused for an attack."

Anyone paying close attention to cybersecurity has known about this threat for years. As James Clapper, former US Director of National Intelligence, told us in 2016: "Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US government systems."

It's no longer "could." We're now living in homes filled with insecure IoT devices.

Why? As Mark Houpt, data center operator DataBank chief information security officer, explained, it's because many IoT devices are inherently insecure for two key reasons: Neglect and the lack of an interface upon which to add security and hardening measures. I mean, exactly how do you control your toothbrush's security setting? How do you add an antivirus program to your refrigerator?

You can't.

So, what ***can*** you do?

Well, for starters, as Zuger said, you can automatically update all your devices whenever an update is available "You can't update enough."

You should also never charge your device at a public USB port. That same port that charges your gadget can also infect it.

I also suggest paying attention if your device suddenly starts losing power faster than normal. Sure, it may just be an aging battery, but it also could be malware running in the background.

You should also be wary of public Wi-Fi connections. The same connection that lets you watch a TikTok may also be loading malware on your smartphone.

While at your home, I urge you to set up a firewall on your Internet connection. If an attacker can't get to your smart toilet, it can't infect it. And, boy, isn't a malware-infected toilet an ugly thought?

Finally -- and I'm quite serious about this -- don't buy an IoT-enabled device unless you have a real need for it. A smart TV? Sure, how else are you going to stream the Super Bowl? But a washing machine, an iron, a toothbrush? No. Just say no.

As we forge ahead into an increasingly connected future, let's ensure that our digital hygiene is as robust as our dental hygiene.

RUSSIAN MILITARY BOTNET DISCOVERED ON 1000+ COMPROMISED ROUTERS

tom’sHARDWARE by Christopher Harper

GRU-funded hacking team Fancy Bear has been caught installing Moobot malware on "well over a thousand" unsecured home and business routers using the default admin password as the infection vector, says FBI Director Christopher Wray [h/t The Register].

Moobot was used to create a functional botnet of compromised routers that the GRU and Fancy Bear were using for undisclosed reasons, but the scale of the security breach isn't promising. The FBI acted to isolate and remove the malware from all infected units. The issue stems from a lack of cybersecurity basics (change the admin password unless you want someone else to change it for you) taught to the public. So, it's not quite like a hardware vulnerability that can't be fixed without revision.

As simple as the root of the issue was (unsecured default admin passwords), the extent of the Moobot malware infection required some pretty big technical steps from the FBI to remove it as a threat. First, they leveraged Moobot's functionality to copy and delete all malicious files, including itself, from the impacted routers. Then, they firewalled all the routers to prevent remote management access (and thus further hijacking) before scrubbing the router's data and inspecting the equipment.

Following the removal of the Moobot malware, the Feds returned the hardware to its original owners, albeit with their settings changes still applied. Users can reset the devices, but the Justice Department warned that "a factory reset that is not also accompanied by a change of the default administrator password will return the router to its default administrator credentials, leaving the router open to reinfection or similar compromises."

In today's era of international cyber attacks and data heists, it's prudent to change the default passwords on your network devices as soon as possible and to safely maintain and change your existing passwords as necessary. It's also a good idea to ensure that your router is running on current firmware that contains the latest security and performance updates. No one wants to unknowingly lose computational, network, or even financial resources to some foreign government, cybercriminal, or creepy neighbor if they can avoid it.

CLUB MEETING and ZOOM

The meeting time is 1100 on Saturday morning at the Lurie Civic Building on the St Petersburg College campus in Seminole. Turn west at the light at 113th St N and about 92nd Ave N. It's the first building on the north side. Here is a link to a Google map: Google Maps . There are a few parking spots in front the Chamber building but double parking is fine since we will be able to find the owner to move his vehicle if necessary. Alternately if you go another 100 yards past you can park in the college parking lot. Below is the Zoom information, same as last month. The ZOOM meeting is limited to 40 minutes so I will start it early and restart it to cover the whole meeting.

Topic: Bill Williams' Zoom Meeting
Time: This is a recurring meeting Meet anytime

Join Zoom Meeting
https://zoom.us/j/2737114584?pwd=d1BETHVOQ21vWWZXZ0lYQ0FlWWtIdz09

Meeting ID: 273 711 4584
Passcode: worm

CLUB NETS

Check in on the club net Thursdays at 1930 and 2000 (or at the end of the 2M net). 2M at 146.850 – with a tone of 146.2. Our 6M net runs after our regular 2M net on 53.150 – 1MHz offset 146.2 tone.

LOCAL NETS

MONDAY

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	28.365 USB	10M 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
1900 146.490 simplex	3RD Tuesday monthly, Hillsborough Co ARES simplex Net	

WEDNESDAY

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 147.165 + 136.5	Humpday Net	from Bandon
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
0000-2359 HF Winlink	Winlink Wednesday Net https://winlinkwednesday.net/reminder.html	

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
1915 224.660- no tone	St Pete ARC	from St Petersburg
1930 146.6385 -127.3	Lakeland ARC	from Lakeland
1930 444.225 + 146.2	Hillsborough ARES/RACES	from Tampa
1930 146.850- 146.2	Wormhole	from Pinellas Co

2000	53.150 –1MHz 146.2	Wormhole	from Pinellas Co
2030	NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

FRIDAY

1830	147.060 no tone	St Pete ARC daily net	from St Petersburg
1900	3.830 LSB	Brandon 80M Net	from Brandon
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 can ask club members for the persons contact information. 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. If you want to see anything here and you are coming to the meeting let the seller know, maybe he can bring it.

FOR SALE,
See Bill AG4QX for the following: most from SK estate, make me an offer.

*Heathkit HD-1215 Phone patch $15 looks ok
*Drake WV-5 wattmeter $90 looks ok
*Wacom WP-604-C low band cans. Can be moded for 6M, talk to Bill

HAMFESTS

2024

April 13 — **TARCFest** TARC Clubhouse, 22nd St at the river, 8AM-1PM, $5 entry including tailgate, a few inside tables must be reserved in advance, talkin on 147.105 +146.2, license testing after, more info at http://hamclub.org/

May 17-19 — **Xenia, Ohio, Dayton Hamfest, ARRL NATIONAL CONVENTION,** tickets $30 at the door, tailgate $30, 10x10 booth $705, https://hamvention.org

May 25 — **WormFest 2024, Pinellas Park, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, southeast corner of US 19 and 49th Street, 33782. Park opens at sunrise for vendor setup, hamfest starts at 0800. Talk-in on 146.850 – 146.2. All FREE! For a map and directions see** http://www.TheWormholeSociety.org **.**

August 24 — **TARCFest** TARC Clubhouse, 22nd St at the river, 8AM-1PM, $5 entry including tailgate, a few inside tables must be reserved in advance, talkin on 147.105 +146.2, license testing after, more info at http://hamclub.org/

December 13 & 14 — **Plant City, the 2024 Tampa Bay Hamfest and West Central Florida Section Convention,** Friday and Saturday**, at the Strawberry Festival grounds, admission $13, 16x40 ft tailgate space $10, electric $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 ;-)**

Last full weekend January	Winter Field Day https://www.winterfieldday.com/
Late January	Gasparilla celebration
Late February	West Central Florida Tech Conference
http://arrlwcf.org/wcf-special-events/wcftechconference/	
March/April	MS Walks
April	MS bike now named Suncoast Challenge
http://www.citrustour.org/register.php	
March/April	Mass Casualty Exercises
Late April	Southeastern VHF Society Conference,
http://www.svhfs.org	
Late April	Florida QSO Party
Mid May	March For Babies (was March of Dimes)
https://www.marchforbabies.org/Registration/Events	
Mid May	Annual Armed Forces Crossband Test
Mid-May	Florida Hurricane Exercise
Late May	Dayton Hamfest
May, Memorial Day Weekend	Wormfest
First weekend in June	Museum Ships on the Air
Fourth weekend in June	Field Day
http://www.arrl.org/contests/announcements/fd/	
Third weekend in August	International Lighthouse/Lightship Week
https://illw.net/	
September	Run for All Children's
October, 3rd weekend	JOTA, Scout Jamboree-on-the-AIR (around 14.280MHz)
Early December	ALS bike ride in Walsingham Park
December, Second weekend	Tampa Bay Hamfest http://www.fgcarc.org/

YOUR WORMHOLE OFFICERS

Bill AG4QX is President and editor of this newsletter, the Vice President position is open, Treasurer is Jim KD4MZL, Paul KA4IOX is the Secretary, Dee N4GD is the Repeater Trustee and Mike KV0OOM is our webmaster.

YOUR WORMHOLE REPEATERS

53.150 –1Mz PL 146.2

442.625 +5Mz PL 146.2

146.850 - 600Kz PL 146.2

The Wormhole 2M and 440 repeaters are both now dual mode Yaesu DR-2X. FM analog as always and Yaesu Fusion, a C4FM digital mode.

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