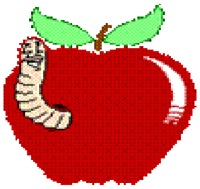
News from



The GLORIOUS SOCIETY OF THE WORMHOLE

March 2020

There will be a regular Wormhole Meeting at the Minreg Center on Saturday March 7th 2020.

If you have any concerns about the COVID-19 virus which has been reported in the Tampa Area, or if you are not feeling 100% yourself , please act accordingly.

Hello Worms

Hello all. I have had a pretty busy month with a bunch of person stuff and then three days in Orlando at the Hamcation. I hope everyone is doing well. I will not make the meeting this month due to working the MS150 Bike Ride. Mike will do his normal bang-up job in my stead. Treat him nice.

The Minnreg building sale to the church has fallen through but now there is a very active situation that might end up making the building a restaurant. So I say again, think about and look for a new Wormhole meeting location. We need somewhere that will accommodate 20 to 30 people and has the place for and will allow cooking, and cheap.

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 FOR THE MEETING IF YOU HAVE ONE. It has been a good while since anyone left a chair!

* ANTI-SOLAR PANEL GENERATES POWER AT NIGHT*

By Ryan Whitwam on February 4, 2020 *EXTREMETECH*

There is free energy raining down on Earth in the form of sunlight, but harnessing all of that energy has proven difficult. The sun only shines during the day, and those solar panels are useless at night, or at least they are right now. Researchers from the University of California Davis suggest you could generate power at night using “anti-solar panels.” Of course, it’s all so obvious when you think about it.

Researchers around the world are working to improve the efficiency of solar panels, which currently only capture a fraction of the total solar energy falling on them. Even high-efficiency solar panels are at a disadvantage compared with non-renewable energy because you can’t generate solar power at night. So, you need to capture enough during the day to store for usage when the sun isn’t shining. However, battery technology has been similarly slow to improve. The anti-solar panels described in the journal ACS Photonicscould fill the gap to supplement power generation at night when solar panels and batteries aren’t good enough.

Solar panels work because they’re cold compared with the sun, so they can absorb sunlight and convert it to energy. Space, and therefore the night sky, is cold. Therefore, you can point a warmer panel on Earth toward the sky to radiate energy outward as infrared light. That’s what the University of California team is proposing—it’s essentially a heat engine.

These devices don’t use the same technology as solar panels, although they’d probably look similar. Solar panels rely on photovoltaic cells that absorb photons to create electron-hole pairs across the semiconductor, generating a working voltage. A nighttime panel would use a thermoradiative cell to emit infrared radiation from the Earth into space to create electron-hole pairs.

The team estimates that thermoradiative cells would only be able to generate about a quarter as much power as a solar panel of the same area. That's mainly a consequence of the lower energy of infrared light. Silicon is the current material of choice for solar panels as it's good at capturing light in the visible wavelengths. It may be possible to boost the efficiency of thermoradiative cells by using materials that can better interact with longer wavelengths of light, for example, mercury alloys.

The University of California study is just an initial proposal for nighttime energy generation. The next step is to start building the devices to see how well they perform.

* SOMEONE HIJACKED A HUGE BOTNET AND IS REMOVING IT*

By Catalin Cimpanu January 23, 2020 *ZDNet*

A mysterious entity appears to have hijacked the backend infrastructure of the Phorpiex (Trik) botnet and is uninstalling the spam-bot malware from infected hosts, while also showing a popup telling users to install an antivirus and update their computers, ZDNet has learned.

The popups have started appearing on users' screens today, early morning, US Eastern time, and have been spotted by the research team at antivirus vendor Check Point. Initially, ZDNet and others thought this was a prank coded inside the malware by the Phorpiex team for the purpose of trolling security researchers analyzing the malware. However, as the hours passed, it became clear that this was actually taking place on customer systems, in the real world, and was not just a popup that was appearing in virtual machines used as malware analysis sandboxes.

"This is truly happening," Yaniv Balmas, Head of Cyber Research at Check Point, told ZDNet. "We are closely monitoring this malware family and have noticed this behavior started just a few hours ago."

Balmas listed several theories as what could have happened -- such as the malware operators deciding to quit and shut down the botnet on their own terms, a law enforcement action, a vigilante security researcher taking matters into his own hands, or a rival malware gang sabotaging the Phorpiex crew by destroying their botnet.

"Hijack seems likely based on the track record for the Phorpiex developer," said a second malware analyst, who declined to have his name used in this article because he was not authorized to speak in his company's name -- another antivirus vendor. "The Phorpiex developer has some pretty nasty rivals in the botnet game so it wouldn't surprise me if this is an attack motivated by jealousy or something along those lines," he added. "The developer for the Phorpiex botnet is extremely lazy and careless," the malware analyst said, claiming that he could have also hijacked the botnet in the past due to its simplistic IRC-based command and control mechanism.

The Phorpiex malware, which has been active for more than a decade, has suffered security breaches in the past, also due to the malware developer's carelessness. In 2018, the Phorpiex developer left one of the botnet's command and control backend servers exposed online, and security researchers were able to retrieve a list of 43.5 million email addresses that the Phorpiex crew was targeting with spam campaigns.

Phorpiex is one of today's most active spam botnets. The Phorpiex team operates by infecting Windows computers and using these systems as spam bots to send out massive spam campaigns. These spam campaigns keep the spam botnet alive, by infecting new PCs with Phorpiex, but they also send out custom spam campaigns on behalf of other cybercrime groups -- the method through which the Phorpiex crew makes its money.

Whoever hijacked the botnet today and instructed bots to uninstall themselves has put a serious dent in the Phorpiex gang's future profits and operations. To give an idea about the size of the profits the Phorpiex crew lost, Check Point previously reported that the same botnet made $115,000 in five months just from mass-spamming sextortion emails.

* RADIO FREQUENCY EXPOSURE TEST FINDS AN IPHONE 11 PRO EXCEEDS THE FCC'S LIMIT*

This item from the Ohio ARRL Section newsletter by way of Tony N2MFT.

http://arrl-ohio.org/news/2020/OSJ-Feb-20.pdf

(Submitted by Gregory Drezdzon, WD9FTZ)

A test by Penumbra Brands to measure how much radio frequency energy an iPhone 11 Pro gives off found that the phone emits more than twice the amount allowable by the U.S. Federal Communications Commission.

The FCC measures exposure to RF energy as the amount of wireless power a person absorbs for each kilogram of their body. The agency calls this the specific absorption rate, or SAR. For a cellphone, the FCC's threshold of safe exposure is 1.6 watts per kilogram. Penumbra's test found that an iPhone 11 Pro emitted 3.8 W/kg.

Ryan McCaughey, Penumbra's chief technology officer, said the test was a follow up to an investigation conducted by the Chicago Tribune last year.

The Tribune tested several generations of Apple, Samsung, and Motorola phones, and found that many exceeded the FCC's limit.

Penumbra used RF Exposure Labs, an independent, accredited SAR testing lab for the tests (The Tribune also used the San Diego-based lab for its investigation). Penumbra was conducting the test, which also included testing an iPhone 7, to study its Alara phone cases, which the company says are designed to reduce RF exposure in a person.

When the FCC conducted a follow-up investigation, they did not find evidence that any of the phones exceed SAR limits. "That said,while the Tribune and Penumbra both used off-the-shelf phones, the FCC largely tested phones supplied by the manufacturers, including Apple," adds IEEE Spectrum.

Joel Moskowitz, a researcher at UC Berkeley, says that could be because there's a systematic problem with RF Exposure Lab's testing methods, or Apple allegedly rigged the software in the provided test phones to ensure they didn't put out enough power to exceed the SAR limit.

Both McCaughey and Moskowitz agree that the FCC’s RF exposure testing is woefully out of date, as the limits reflect what the FCC deemed safe 25 years ago.

Read the IEEE Spectrum report at:https://spectrum.ieee.org/tech-talk/telecom/wireless/radio-frequency-exposure-test-iphone-11-pro-double-fcc-limits

* MORE BAD APPS FROM GOOGLE PLAY*

by Liviu Arsene and Alexcandra Bocereg, *Bitdefender Reseaerch*

Bitdefender researchers recently found 17 Google Play apps that, once installed, start hiding their presence on the user's device and constantly display aggressive ads. While not malicious per se, the tactics they use to smuggle themselves into Google Play and dodge Google's vetting system are traditionally associated with malware.

Waiting 48 hours before hiding their presence on the device, splitting the app's code into multiple resource files, and holding off displaying ads until 4 hours after app installation are among the tactics these developers use to plant their apps onto Google Play. With over 550,000 downloads in total, the apps found have flown below the radar of Google's vetting system mostly because they also delivered on their promise: they do what they say they do.

At the time of writing, Google has been notified and the reported apps are being taken offline.

The description for one of the apps analyzed involves enticing users with a racing simulator that also offers in-app payments for extra in-game features. While the gaming part works just fine, the app shows popup ads when the user is not playing the game and hides for some time following the installation. The ads are displayed at random time intervals, making it hard for users to recognize a pattern of when ads are shown.

Users see multiple ads either in-game when pressing different buttons or even if not in the app. The frequency at which ads appear while in the game depends on a random value. In half the cases, there is a probability that when using some game functionalities, an ad pop ups.

The ad-showing mechanisms are scattered around the application, within multiple activities, and using modified adware SDKs. The randomness of ad occurrences and display time intervals is modified by the developer to decrease the likelihood of users noticing any patterns.

One method for the app to dodge Google Play checks is by waiting 48 hours to hide. The code is also split in two dex files, making it difficult for security researchers to grasp the logic of the app. Another technique used is to manipulate the broadcast receiver for android.intent.action.USER_PRESENT to display ads only after 4 hours following installation.

The app also comes with game-related .so files that are not used. These library files are common in Android games, as they provide fast graphics rendering on a mobile environment with limited resources. What is interesting here is that the game actually uses the other .so files found in an archive within the assets directory, despite already having them in the lib directory. This could be a mechanism intended to make the app give the impression of being an average game, while its main purpose is to aggressively display ads.

In other versions, including versions that were at some point on Google Play, requests to the ad web sites also contain sensitive information about the user, such as phone model, IMEI, IP address, MAC address, and location information. Some apps have no second dex and have all the functionality in the initial one.

Some users that have tried the apps left reviews that raised warning signs about the apps' behavior. While some users were irked that they couldn't even play the game because of full screen ads, other complained of battery drainage and accurately identified an app's dubious hiding behavior after installation.

The methods described above to dodge Google's vetting system seem to have been put to good use, as Bitdefender researchers have identified 17 other apps that share the same practices. While the creators' and applications' names are different, they all share the same features in terms of hiding their existence and displaying ads.

While the Google Play apps found are not tagged as malware, but more as Riskware, users are strongly encouraged to always have a security solution installed on their devices, as it can accurately identify these apps and prevent users from installing them. Whether downloaded from official or third-party marketplaces, a mobile security solution will keep users safe from malware, riskware, or other potentially malicious apps as well as phishing or fraudulent websites. Bitdefender identifies the found samples using the following detections: *Android.Riskware.HiddenAds.HH, Android.Riskware.HiddenApp.AX, Android.Riskware.HiddenApp.HU*.

Editors Note: To see the list of apps goto https://labs.bitdefender.com/2020/01/seventeen-android-nasties-spotted-in-google-play-total-over-550k-downloads/

* ZERO DAY BUG IN CHROME*

There is a serious zero day bug in Chrome that was probably updated automatically but to check see the following from the Google website. My icon is grey so I am good. If you regularly use Chrome then it should have updated several weeks ago. I did say should have. It is a computer so it can screw up faster than ….. well fast!

Get a Chrome update when available

Normally updates happen in the background when you close and reopen your computer's browser. But if you haven't closed your browser in a while, you might see a pending update:

1. On your computer, open Chrome.
2. At the top right, look at More ⋮.
3. If an update is pending, the icon will be colored:
    - Green: An update was released less than 2 days ago.
    - Orange: An update was released about 4 days ago.
    - Red: An update was released at least a week ago.

To update Google Chrome:

1. On your computer, open Chrome.
2. At the top right, click More ⋮.
3. Click Update Google Chrome.
    - Important: If you can't find this button, you're on the latest version.
4. Click Relaunch.

The browser saves your opened tabs and windows and reopens them automatically when it restarts. Your Incognito windows won't reopen when Chrome restarts. If you'd prefer not to restart right away, click Not now. The next time you restart your browser, the update will be applied.

Bill

CLUB MEETING

The next club meeting is March 7th. 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 fence 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 our 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 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. 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

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

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
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 St Petersburg
2000 53.150 –1MHz 146.2	Wormhole	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, ICOM **IC-756 Pro**, HF and 6M, 100 watts, hand mic, power cord and manual, Local only. See George W1AAG

HAMFESTS

March 7 Punta Gorda, Charlotte County Hamfest, Punta Gorda Boat Club, 802 West Retta Esplanade, talk-in on 147.255 + 136.5, contact David Beck, WB4GVZ at a1steel@verizon.net or 804-363-0894

March 14 New Port Richey, Gulf Coast ARC Spring Hamfest, Millennium Academy, 10005 Ridge Road, For info see http://gulfcoastarc.org/2020/02/27/gcarc-hamfest-come-on-down/

March 21 Zephyrhills, ZAARC Hamfest, St. Elizabeth Episcopal Church, 5855 15th St., $5 entry or tailgate, For info see https://www.zaarc.org/2020_Hamfest.pdf or e-mail ke7uth@arrl.net

March 28 Odessa, Pasco Co Spring Hamfest, Gunn Hwy Flea Market, 2317 Gunn Hwy, no info on website, contact Don KA2KDP at 727-868-0176 or email n9ee55@gmail.com

March 28 Sarasota, Sarasota ERC, American Red Cross, 2001 Cantu Court, $2 entry, $5 tailgate, $15 inside, limited space, for info e-mail SERC@comcast.net

April 18 **TARCFest** TARC Clubhouse, 22nd St at the river, $5 entry including tailgate, a few inside tables reserved in advance, talkin on 147.105 +146.2, more info at http://hamclub.org/

May 23 **WormFest 2020, 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 442.625 + or 146.850 – both with a tone of 146.2. For a map and directions see** http://www.TheWormholeSociety.org **.**

June 13 Dade City, Pre-ARRL Field Day Tail-Gators' Gathering, Dade City Masonic Lodge, 13642 21st St So, for info contact Gary Mentro , N3OS, 813-713-9994 or n3os@arrl.net

August 22 **TARCFest** TARC Clubhouse, 22nd St at the river, $5 entry including tailgate, a few inside tables reserved in advance, talkin on 147.105 +146.2, more info at http://hamclub.org/

November 9 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 https://www.sparc-club.org/sparcfest/

December 11 & 12 **Plant City, the 2018 Tampa Bay Hamfest is the Florida State Convention and 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	Adventure Run, Honeymoon Island
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/	
Late February	MS 150 Citrus Tour bike ride
http://www.citrustour.org/register.php	
March/April	MS Walks
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

May, Memorial Day Weekend	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, 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

53.150 –1Mz PL 146.2

442.625 +5Mz PL 146.2

146.850 - 600Kz 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 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