MARANews

May 2021
Volume 59 Issue 5

http://www.w1mv.org https://www.facebook.com/w1mvmara/

https://twitter.com/search?q=Massasoit%20Amateur%20Radio%20Association&src=typd

Next meeting is May 18, 2021 at 6:30 at the EOC in Bridgewater.

Membership
The website has been updated with our current roster of paid members. If there are corrections, please drop an email to maranews@w1mv.org

Presidents Notes
MARA Facebook page: Our Massasoit Amateur Radio Association Facebook page with club events, meetings, photos, etc. are occasionally updated so that it may be another resource for us on which to spark interest in our club, amateur radio and keep members informed of what we are doing outside of our club meetings and in our community. If you go to the "about" tab on our page you can find our http://www.w1mv.org/ web page for our present and past newsletters and other club information. Please send Phil N1XTB n1xtb@powersrvcs.com or Wendy KC1GTR kc1gtr.mara.@gmail.com any articles or photos you would like to see in our MARA newsletter, W1MV-MARA Website and Facebook page. Jeff - AJ1L has created a link to twitter to help get the word out even more!

Secretary's Notes - MARA Meeting 04/20/2021 – Wendy White-KC1GTR

Zoom Meeting

Open: WA1BEE - Allen Hiltz called the meeting to order at 7:00pm

Attendance: Allen - WA1BEE, Phil N1XTB, Jeff AJ1L, Tom Luckman - WA1TOM, Barry N4NMF, Richard AG1B

President - Allen Hiltz - WA1BEE **Vice President** – Jeff Lehmann – AJ1L

Secretary– Wendy White – KC1GTR **Treasurer** - Phil McNamara - N1XTB

Secretary Notes - KC1GTR - Wendy White – last month's notes were ok as is. Motion to approve made by Tom – WA1TOM, Richard – AG1B seconded the motion. All in favor, 0 opposed.

Club Treasurer Report – Phil gave the treasures report. Membership dues have not been paid by a few members. We currently have 18 plus 2 more that are sending in their dues. Need to

work on this. Motion to accept Treasurer's report was made by Tom WA1TOM and the motion was seconded by Tom WA1TOM All in favor, 0 opposed.

Repeater Report – Jeff AJ1L – All is good –working on the ongoing issue, nothing else is happening. Tom WA1TOM made a motion to accept. Richard AG1B seconded. All in favor, o opposed.

Current Business – Looking for ways to increase membership and we were all in favor of holding a 50/50 raffle at the next in person meeting. Send out announcements and we can post this on our facebook page and along with that our Venmo Acct information. Richard AG1B made the motion to accept the raffle, Barry N4NMF seconded the motion. All in favor, 0 opposed.

Allen – WA1BEE is looking for suggestions for ideas on having a public event, increase awareness. Bring go bags, set them up and explain what is in the bag. A few advanced HAMS have great go kits that they could share.

Tom WA1TOM will have the EOC open at 6:30pm for meet and greet. The meeting will start at 7:00pm on May 18th at the Bridgewater EOC. Jeff will get the map to Wendy for the newsletter.

Tom WA1TOM made a motion to close the meeting and Barry N4NMF seconded the motion. All in favor, 0 opposed. Allen closed the meeting at 7:41pm

HAM RADIO LOCAL AREA NETS

Any additions or corrections contact John – N1UMJ at: N1UMJ@arrl.net.
All Frequencies are in MHz and 6 Meters (50.0 MHz and up.) are FM Mode unless otherwise noted.

Sunday:

8:30 AM WA1NPO – WARPSN Net, Whitman ARC Rptr, 147.225 +, PL 67.0 8:45
AM New England phone net, 3.945 +/--- LSB

Daily:

7:00 PM NE Cracker Barrel Net, Matt – W1AEM, NCO, 3.921.00 MHz LSB Pilgrim Amateur Wireless Assoc. 10 Meter Net
7:00 PM 28.375.0 USB Cape & Island Traffic Net, Mon. Tue. Thur.
7:00 PM Plymouth N1ZIZ Rptr, 146.685 – PL 131.8
7:30 PM Falmouth N1YHS Rptr, 147.375 + PL 110.9 Genesis ARC CW Training Net
8:00 PM Eastern MA 2 Mtr Traffic Net, Boston W1BOS Rptr, 145.230 – PL 88.5

8:00 PM Norfolk County Radio Association Net, , Walpole Rptr, 146.895 – PL 123.0

Monday:

6:00 AM Cape and Islands Weather Net, M-S, Dennis K1PBO Rptr, 146.955 – PL 88.5
8:00 PM Fairhaven Weather Net, SEMARA Rptr, 147.000 + PL 67.0
8:00 PM Norfolk County Emergency Preparedness Net, Walpole Rptr, 146.895 – PL 123.0
8:30 PM New England DMR net, DMR---MARC repeaters talk group 3181 New England Falmouth ARA Net, Falmouth K1RK Rptr, 146.655 – PL 88.5
9:00 PM Boston ARC Rag Chew Net, Boston W1BOS Rptr, 145.230 – PL 88.5

Tuesday:

7:30 PM Plymouth N1ZIZ Rptr, 146.685 – PL 131.8
8:00 PM Fairhaven Weather Net, SEMARA Rptr, 147.000 + PL 67.0
8:00 PM Massasoit ARA Net, , Bridgewater W1MV Rptr, 147.180 + PL 67.0 (Except 3rd Tue!) Genesis ARC 2 Mtr Rag---Chew Net,
8:00 PM Norwood Amateur Radio Club Net, Norwood Rptr, 147.210 + PL 100.0 220 MHz Day! Try to find a 220 Repeater near you and give a call out!

Wednesday:

7:00 PM Blackstone Valley ARC, 2 Mtr Simplex Net, 146.565
8:00 PM Cape and Islands ARES Net, Dennis K1PBO Rptr, 146.955 – PL 88.5
8:00 PM Fairhaven Weather Net, SEMARA Rptr, 147.000 + PL 67.0
8:00 PM Whitman ARC 10 Meter Rag---Chew Net, 28.333.0 USB - Except 1st Wed!
9:00 PM Waltham Wranglers Swap Net., Waltham W1MHL Rptr , 146.64 – PL 136.5

Thursday:

7:00 PM Genesis ARC CW Training Net, Plymouth N1ZIZ Rptr, 146.685 – PL 131.8 10 Mtr
8:00 PM Fairhaven Weather Net, SEMARA Rptr, 147.000 + PL 67.0
8:00 PM General Class Rag---Chew Net, 29.470.0 FM
8:30 PM Sturdy Mem. Hosp. ARC ARES Prac Net, K1SMH Rptr, 147.195+ PL 127.3 900 MHz

Friday:

8:00 PM Fairhaven Weather Net, SEMARA Rptr, 147.000 + PL 67.0
8:00 PM Great Hill Swap Net, K1USN, 145.390 and Echollink/Irpl 9127

Saturday:

8:00 PM South Shore Skywarn Net, Bridgewater W1MV Rptr, 147.180 + PL 67.0

VKEMCOMM Echolink Conference node: 270177/IRLP 9508 (due to *WX---TALK* Echolink conference node: 7203/IRLP 9219 outage) Refer to: http://www.voipwx.net/

MARANews

Massasoit Amateur Radio Association Executive Board

President - Allen Hiltz - WA1BEE
Vice President Jeff Lehmann – AJ1L
Secretary Wendy White – KC1GTR
Treasurer: Phil McNamara N1XTB
Call Sign Trustee: Phil McNamara N1XTB

2M Repeater	147.180+ (Tone 67.0)
440 Repeater	444.550+ (Tone 88.5)
APRS Node	Node 144.39 W1MV-1
Packet BBS	145.09 N1XTB-4
Packet Node Brockton	145.09 W1JOE-7 (BROCK)
MARA Web Page	http://www.w1mv.org/
Facebook	https://www.facebook.com/w1mvmara/
Newsletter Editor	kc1gtr.mara@gmail.com
ARC Web Page	http://www.wa1npo.org
Qsl via	www.eqsl.cc
Skywarn	http://wx1box.org and www.powersrvcs.org/w1gmf/skywarn.htm
Mailing Address	P.O. Box 428 Bridgewater, MA 02324

Monthly meetings are held the 3rd Tuesday of each month, for time being, Tuesday Night Zoom meeting will be at 7:00pm. Allen will advise if we can go to in person for next month's.

Our **Meetings-On-The-Air** are held all other Tuesday evenings at 8PM on 147.180+ and includes the Westlink News Report with the latest news about happenings in the world of Amateur Radio.

The **South Shore Skywarn Net** is held every Saturday evening at 8PM local time on 147.180+ and is open to all hams.

VE Exams are held the 2nd Saturday of every month, in Braintree contact Steve Cohen, W1OD via email w1od@arrl.net. Walk-ins are no longer permitted. We will be hosting VE exams at 8:45 at the Watson building. If you know of anyone planning to take an exam, please have them drop a note to Steve to confirm a reservation.

http://www.hamradiolicenseexam.com/index.html

MARANews

The K7RA Solar Update

05/14/2021

Tad Cook, K7RA, Seattle, reports: Sunspot activity returned last Friday, May 7, and has held steady since. Average daily sunspot numbers rose from 11.9 to 21.1, and average daily solar flux was up 2.1 points to 74.3 for the reporting week ending May 12.

Geomagnetic activity was quiet until Wednesday, May 12, when the planetary A index went to 41 as the result of a coronal mass ejection (CME) that blasted out of the sun on May 9. It was not expected to be very strong, but when it struck on May 12, it sparked a G3 class geomagnetic storm — the strongest in the current solar cycle.

The planetary A index rose to 41, far above an average of 3.8 on the previous 6 days. The average daily planetary A index for the May 6 – 12 reporting week was 9.1 and average middle – latitude A index was 7.4.

Predicted solar flux over the next month is 75 on May 14 – 19; 70 on May 20 – 21; 72, 80, and 79 on May 22 – 24; 78, 77, and 73 on May 25 – 27; 72 on May 28 – 30; 70 on May 31 and June 1; 71 and 75 on June 2 – 3; 76 on June 4 – 5; 74 on June 6 – 7; 75 on June 8 – 9; 77 on June 10, and 79 on June 11 – 13.

The predicted **solar flux** of 84 on June 15 in the 45-day forecast seems to be an outlier. It's odd that predicted solar flux would shift from 78 to 84 to 77, but we saw a **similar prediction** recently for that same value a week into the future. Any trace of it here seems to have disappeared down the memory hole.

Predicted planetary A index is 5 on May 14 – 16; 15, 12, 8, 5, and 8 on May 17 – 21; 5 on May 22 – June 5; 8, 5, and 8 on June 6 – 8, and 8, 5, 12, 18, and 15 and on June 9 – 13.

Here's the geomagnetic activity forecast for May 14 – June 8 from F.K. Janda, OK1HH, of the Czech Propagation Interest Group, which has been compiling weekly geomagnetic activity forecasts since January 1978.

The geomagnetic field will be:

- quiet on: May 19, 25-26, (27-31)
- quiet to unsettled on: May 21, 24, 31, June 1-8
- quiet to active on: May (14-16, 18, 20-23)
- unsettled to active: May (17)
- active to disturbed: none
- Solar wind will intensify on: May (16,) 17-18, (21-25,) 28-30

Remarks:

- Parenthesis means lower probability of activity enhancement.

- Contradictory indications significantly reduce forecast accuracy.

Jon Jones, N0JK (EM28), wrote: “6-meter E skip to W6 on May 14 to Silicon Valley. Worked AH0U and N5KO, both in CM97. They are in the sporadic E ‘doughnut’ between single and double hop Es.”

Ken Brown, N4SO, checks this **graph of the EISN** — the estimated international sunspot number — a daily value obtained by a simple average over available sunspot counts from 85 world-wide observers in the SILSO network and, “compares it with propagation on 30 and 17 meters. Of interest are stations in China, Japan, Korea, and Asiatic Russia propagated at 6,000 miles plus.” Also see the **SIDC/SILSO International Sunspot Number**.

Ken also reported that on May 11, the W1AW code practice bulletin on 17 meters were 40 dB over S-9. “So I called CQ QRP.” He had the power set all the way down on his Elecraft K2, which is 100 mW. He heard or worked W3UA, KM3T, and at 3 W worked K7QO. On FT8 on 30 meters, he worked “a long string of Japanese stations” from 0745 until 1114 UTC — 26 stations in all. The strongest were JE0ART (–3 dB) and JA1IOA (+5 dB) over a roughly 7,000-mile path.

The Reverse Beacon Network (RBN) on 10 meters showed KC0VKN (Iowa) in QSO with K4SE (Tennessee) at 1043 UTC on May 11.

This article, “Using Sporadic E, Es Propagation for Amateur Radio” in *Electronics Notes*, was mentioned in ***The ARRL Contest Update*** newsletter for May12. Then visit the **propquest page** for an interesting online real-time sporadic-e tool.

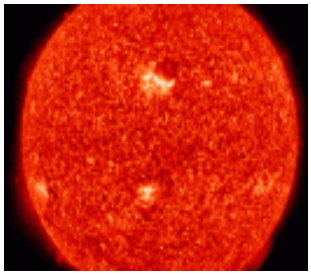
Here are two recent reports [**1**] [**2**] from Space Weather Woman Tamitha Skov, WX6SWW.

Sunspot numbers for May 6 – 12 were 0, 15, 17, 18, 36, 31 and 31, with a mean of 21.1. The 10.7-centimeter flux was 70.8, 74.5, 71.6, 75.9, 76.5, 76.1, and 74.7, with a mean of 74.3. Estimated planetary A indices were 4, 3, 3, 4, 6, 3, and 41, with a mean of 9.1. Middle latitude A index was 2, 3, 4, 6, 8, 4, and 25, with a mean of 7.4.

For more information concerning radio propagation, **visit** the ARRL Technical Information Service, **read** “What the Numbers Mean…,” and **check out** K9LA’s Propagation Page.

A propagation bulletin **archive** is available. For customizable propagation charts, visit the **VOACAP Online for Ham Radio** website.

Photo Gallery



MARANews

Courtesy of IARU

Amateur Radio Through the Decades

1900 – 1910: Following in the footsteps of Marconi and other pioneers, thousands of young experimenters built simple "spark" transmitters and receivers to send Morse code messages around their neighborhoods — sometimes causing interference to commercial and military communications.

1910 – 1920: To address the interference problem, licensing was introduced in 1912. Amateurs began to organize themselves into clubs, forming the basis for today's national associations in Australia (1910), Great Britain (1913), and the United States (1914). The World War caused amateur stations to be shut down but led to advances in radio technology that were quickly adopted by amateurs, once allowed back on the air, in their quest to span greater distances.

The Twenties: Vacuum tube (valve) technology replaced spark, reducing interference and increasing range. The remarkable properties of the ionosphere were harnessed by amateurs to achieve global communication using relatively low transmitter power and antennas that could fit in a typical backyard. To retain access to "short wave" spectrum amateurs had to overcome pressure from commercial and government interests; the IARU was created for that exact purpose. Morse code remained the dominant mode used by amateurs despite the growth of AM broadcast listening.

The Thirties: Amateur radio grew during the Depression as an inexpensive and productive pastime. It became possible to contact amateurs in 100 different countries, even though there were fewer countries then. Television and the exploration of VHF spectrum occupied the attention of the cutting-edge technologists while others built their own AM transmitters and voice communication became popular. Propaganda broadcasting impacted the short waves, creating a new challenge to amateur spectrum access.

The Forties: World War Two caused amateur radio to be shut down in most countries. Once again, technology was advanced by wartime need. After the war, surplus radio equipment was plentiful and inexpensive. This allowed amateurs to upgrade their stations and for the first time to explore UHF and microwaves. A new mode, radioteletype (RTTY), began to be heard on the amateur bands as a result of the surplus bonanza.

The Fifties: Television broadcasting posed a challenge for amateurs, requiring new diplomatic and technical skills to address "TVI" (television interference) to their neighbors' and families' sets. In spite of this it was a decade of rapid growth. Single sideband (SSB) dramatically increased the efficiency and reduced the necessary bandwidth of voice communication. Mobile operation became popular. Toward the end of the decade a peak in the sunspot cycle gave amateurs the best ionospheric propagation ever experienced, before or since. Amateurs tuned into the first signals from space after the first Sputnik was launched. Heathkits, complete sets of components with step-by-step instructions for assembly, captured a large share of the equipment market.

The Sixties: Amateur radio officially joined the Space Age with the first amateur-built satellites. Amateur two-way communication by reflecting signals off the moon (Earth-moon-Earth, or EME) was achieved, first on 1296 MHz and later on 144 MHz. Back on Earth, SSB became the dominant HF voice mode. Separate HF transmitters and

receivers began to disappear from amateur stations, replaced by transceivers with many circuits shared between the two functions. Good equipment from Japan began appearing in ham shacks throughout the world. Some countries began to issue licenses for VHF and higher frequencies without requiring Morse code ability.

The Seventies: Long-duration satellites made satellite communication a permanent feature for space-minded amateurs. Bolstered by a large domestic market, Japanese manufacturers became dominant globally. VHF and UHF repeaters surged in popularity, extending the range of mobile FM equipment. In the mid-70s the "CB boom" became the biggest source of newly licensed radio amateurs as more-serious hobbyists fled the chaos of the Citizens Band. The decade ended with the important World Administrative Radio Conference (WARC-79) where the many years of work by the IARU led to successful defense of existing amateur bands and new allocations at 10, 18, and 24 MHz.

The Eighties: Microprocessors became the vehicle for rapid development of the digital dimension of amateur radio. Propelled by the adoption of a standard for digital data communication known as AX.25, "packet radio" became a powerful new tool for message forwarding. Another adaptation of a commercial standard, known in its amateur version as AMTOR, brought error-free data communication to the HF bands. The manned space program entered ham shacks around the world as amateurs were able to communicate directly with an astronaut aboard the Space Shuttle in Earth orbit, the first of many to follow on the International Space Station.

The Nineties: Dramatic political events in eastern Europe led to significant changes for radio amateurs there. Globally the Internet represented both a challenge and an opportunity: competition for the time and attention of technologically minded youth on the one hand, an unprecedented medium for information exchange on the other. The digital revolution continued to fuel amateur radio development; few ham shacks were without at least one personal computer integrated into the station. PSK31, a digital mode designed specifically for amateur radio use and not based on a commercial standard, offered weak-signal performance and narrow bandwidth comparable to CW.

The 2000s: The introduction of WSJT, a suite of open-source programs designed for weak-signal digital communication by amateur radio, spurred a wave of propagation observation and investigation using techniques adapted from radio astronomy. Digital voice became popular. Software defined radios (SDRs) offered capabilities that were unimaginable just a few years earlier, at prices amateurs could afford. The 2007 World Radiocommunication Conference (WRC-07) made the first-ever low frequency (LF) amateur allocation at 136 kHz.

The next two WRCs, in 2012 and 2015, allocated new amateur bands at 472 kHz and near 5 MHz respectively. WRC-19 adopted a dramatic improvement of the amateur 50 MHz band in Region 1, providing a degree of global harmonization in this intriguing part of the spectrum.

The amateur experimenters of a century ago would be amazed at what amateurs can do today — and there's more to come!

MARANews

Cybersecurity recent events brings back to mind many large scale attacks. Are they driving pricing up? Gas is now almost $3.00/Gallon…..

10 of the biggest cyber attacks of 2020

Here is a list of 10 of the largest cyber attacks of a pandemic-dominated 2020, including several devastating ransomware incidents and a massive supply chain attack.

By Arielle Waldman, News Writer

Published: 05 Jan 2021

A pandemic-focused year made the events of 2020 unprecedented in numerous ways, and the cyber attacks were no different.

As the world transitioned to virtual everything -- work, school, meetings and family gatherings -- attackers took notice. Attackers embraced new techniques and a hurried switch to remote access increased cyberthreats across the board. For example, K-12 schools took a brunt of the hit, and new lows were reached like the exfiltration of student data. The list of top cyber attacks from 2020 include ransomware, phishing, data leaks, breaches and a devastating supply chain attack with a scope like no other. The virtually-dominated year raised new concerns around security postures and practices, which will continue into 2021.

While there were too many incidents to choose from, here is a list of 10 of the biggest cyber attacks of 2020, in chronological order.

1. **Toll Group**

Toll Group tops the list for the year's worst cyber attacks because it was hit by ransomware twice in three months. However, a spokesperson for Toll Group told SearchSecurity the two incidents were not connected and were "based on different forms of ransomware." On Feb. 3 the Australia-based logistics company announced on Twitter that it had suffered a cyber attack. "As a precautionary measure, Toll has made the decision to shut down a number of systems in response to a cyber security incident. Several Toll customer-facing applications are impacted as a result. Our immediate priority is to resume services to customers as soon as possible," Toll Group wrote on Twitter. The most recent attack occurred in May and involved a relatively new ransomware variant: Nefilim.

2. **Marriott International**

For the second time in two years, the popular hotel chain suffered a data breach. On March 31, Marriott released a statement disclosing the information of 5.2 million guests was accessed using the login credentials of two employees at a franchise property. According to the notice, the breach affected an application used by Marriott to provide guest services. "We believe this activity started in mid-January 2020," the statement said. "Upon discovery, we confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests." While the investigation is ongoing, Marriott said it has no reason to believe that the information included the Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers. However, compromised information may have involved contact details and information relating to customer loyalty accounts, but not passwords.

Marriott suffered another major data breach in early 2020, the second such breach for the hotel chain in two years.

3. **Magellan**

On May 12, the healthcare insurance giant issued a letter to victims stating it had suffered a ransomware attack. Threat actors had successfully exfiltrated logins, personal information and tax information. The scope of the attack included eight Magellan Health entities and approximately 365,000 patients may have been impacted. "On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email on April 6 that impersonated a Magellan client," the letter said. The company, which has over 10,000 employees, said at the time of the letter they were not aware of any fraud or misuse of any of the personal information. Phishing, a common attack vector, intensified over the year as threat actors refined their impersonation skills.

4. **Twitter**

The popular social media company was breached in July by three individuals in an embarrassing incident that saw several high-profile Twitter accounts hijacked. Through a social engineering attack, later confirmed by Twitter to be phone phishing, the attackers stole employees' credentials and gained access to the company's internal management systems; dozens of high-profile accounts including those of former President Barack Obama, Amazon CEO Jeff Bezos, and Tesla and SpaceX CEO Elon Musk, were hacked. The threat actors then used the accounts to tweet out bitcoin scams that earned them over $100,000. Two weeks after the breach, the Department of Justice (DoJ) arraigned the three suspects and charged 17-year-old Graham Ivan Clark as an adult for the attack he allegedly "masterminded," according to authorities.

5. **Garmin**

The navigation tech supplier suffered a cyber attack that encrypted some of its systems and forced services offline. Though Garmin first reported it as an outage, the company revealed on July 27 that it was the victim of a cyber attack which resulted in the disruption of "website functions, customer support, customer-facing applications, and company communications." The press release also stated there was no indication that any customer data was accessed, lost or stolen. Speculation rose that the incident was a ransomware attack, although Garmin never confirmed. In addition, several media outlets reported that they gave in to the attackers' demands, and a ransom had been paid. Some news outlets reported it as high as $10 million.

6. **Clark County School District**

The attack on the Clark County School District (CCSD) in Nevada revealed a new security risk: the exposure of student data. CCSD revealed it was hit by a ransomware attack on Aug. 27 which may have resulted in the theft of student data. After the district declined to pay the ransom, an update was posted saying it was aware of media reports claiming student data had been exposed on the internet as retribution. While it's unclear what information was, the threat of exposing stolen student data was a new low for threat actors and represented a shift to identity theft in attacks on schools.

7. **Software AG**

The German software giant was the victim of a double extortion attack that started on Oct. 3, which resulted in a forced shutdown of internal systems and ultimately a major data leak. Files were encrypted and stolen by operators behind the Clop ransomware. According to multiple news outlets, a $20 million ransom was demanded, which Software AG declined to pay. As a result, the ransomware gang followed through with its promise and published confidential data on a data leak site including employees' passport details, internal emails and financial information. Operators behind the Clop ransomware weren't the only group utilizing a double extortion attack. The name-and-shame tactic became increasingly common throughout 2020 and is now the standard practice for several ransomware gangs.

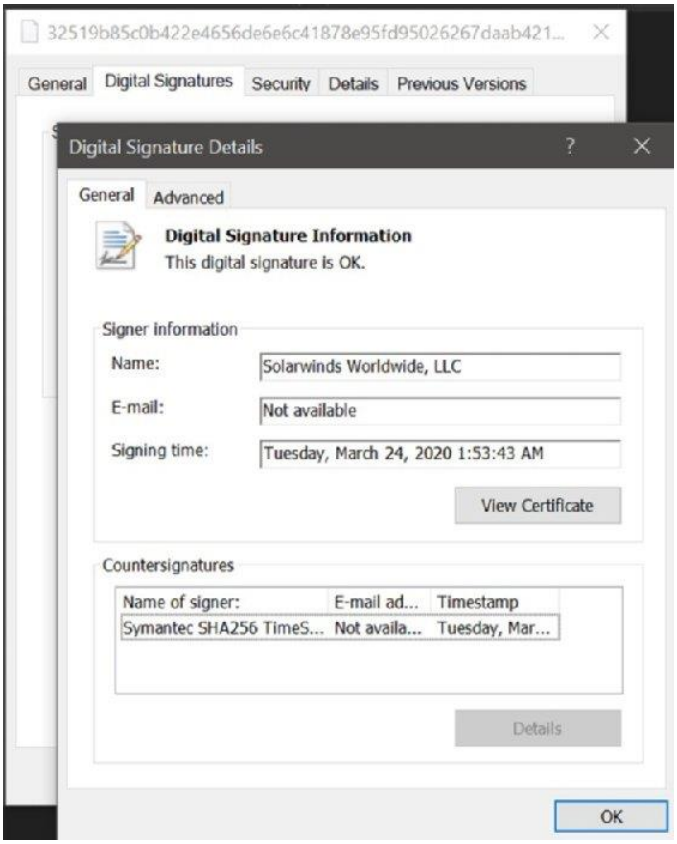
8. **Vastaamo Psychotherapy Centre**

The largest private psychotherapy provider in Finland confirmed it had become the victim of a data breach on October 21, where threat actors stole confidential patient records. The attack set a new precedent; rather than making demands of the organization, patients were blackmailed directly. As of last month, 25,000 criminal reports

had been submitted to Finland police. In addition, the government's overall response to the incident was significant, both in urgency and sensitivity. Finland's interior minister called an emergency meeting with key cabinet members and provided emergency counseling services to potential victims of the extortion scheme.

9. **FireEye and SolarWinds supply chain attack victims**

FireEye set off a chain of events on Dec. 8th when it disclosed that suspected nation-state hackers had breached the security vendor and obtained FireEye's red team tools. On Dec. 13, the company disclosed that the nation-state attack was the result of a massive supply chain attack on SolarWinds. FireEye dubbed the backdoor campaign "UNC2452" and said it allowed threat actors to gain access to numerous government and enterprise networks across the globe. According to a joint statement Dec. 17 by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency and the Office of the Director of National Intelligence, the attacks are ongoing. Additionally, the statement revealed that the supply chain attack affected more than just the Orion platform. CISA said it has "evidence that the Orion supply chain compromise is not the only initial infection vector leveraged by the APT actor." Since the statement, major tech companies such as Intel, Nvidia and Cisco disclosed they had received the malicious SolarWinds updates, though the companies said they've found no evidence that threat actors exploited the backdoors and breached their networks. However, Microsoft disclosed on Dec. 31 that threat actors infiltrated its network and viewed -- but did not alter or obtain -- the company's source code. Microsoft also said there is no evidence the breach affected customer data or the company's products and services.



Nation-state threat actors placed a backdoor in software updates for SolarWinds' Orion platform.

10. **SolarWinds**

The scope of the attack, the sophistication of the threat actors and the high-profile victims affected make this not only the biggest attack of 2020, but possibly of the decade. The incident also highlights the dangers of supply chain attacks and brings into question the security posture of such a large company. Threat actors, who had performed reconnaissance since March, planted a backdoor in SolarWinds' Orion platform, which was activated when customers updated the software. SolarWinds issued a security advisory about the backdoor which the vendor said affected Orion Platform versions 2019.4 HF5 through 2020.2.1, which were released between March 2020 and June 2020. "We have been advised this attack was likely conducted by an outside nation-state and intended to be a narrow, extremely targeted and manually executed attack, as opposed to a broad, system-wide attack," the company said. In the three-week-long investigation since, the full breadth of the attack has grown immensely, but is still not yet fully understood.

Courtesy of K1USN Happenings

Virtual Contest Super Suite - Wednesday May 19
By K3LR, Tim Duffy

All are invited to the Virtual Contest Super Suite hosted by Val, NV9L. **It is free!**

Starting at 7:59 PM on Wednesday May 19, 2021 (2359 Zulu)

Many breakout rooms - lots of virtual fun at the Super Suite

The link you click on to get access to the Suite is here:
https://www.contestuniversity.com/

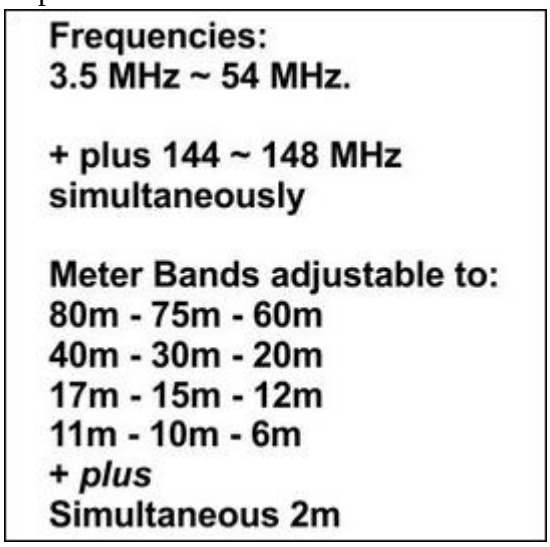
Don't forget to register for Contest University and Hamvention Forums!

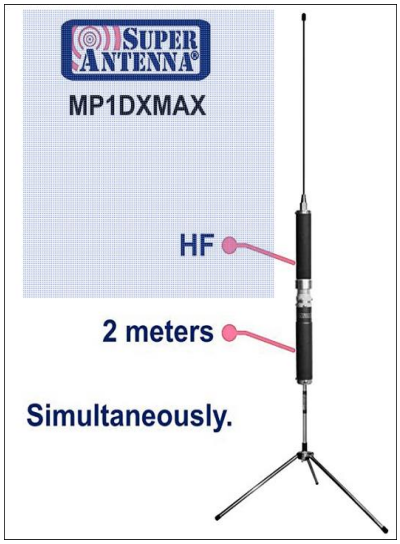
They are free!

Hope to see you at the Virtual Contest Super Suite - bring your own pizza!

MARANews

Super Antenna





Amateur Radio Satellites - Updated by IARU Satellite Frequency Coordination Panel - CubeSats being deployed are:

- GuaraniSat-1 (BIRDS-4)
- RSP-01
- TAUSAT-1
- Maya-2 (BIRDS-4)
- WARP-01 • OPUSAT-II
- STARS-EC
- Tsuru BIRDS-4)
- OPUSAT-II

BIRDS-4 satellites are carrying digipeaters and TAUSAT-1 has an FM transponder. Further information including the IARU coordinated frequencies are at http://amsat.org.uk/iaru/