ARES COMMUNICATOR

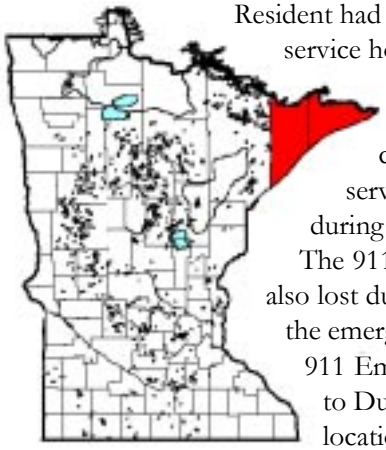
Information for Scott County Amateurs

March, 2010 | **Accurate, Reliable Emergency Communications** | *Volume 10, Number 3*

Lake County Outage

A communications black-out hit Lake and Cook Counties in northeastern Minnesota for about twelve hours on January 26th. Telephone and internet service to the area relies upon a fiber optic cable that travels through Duluth on it's way to the north shore.

Initially reports indicated the fiber optic cable was damaged when a steam pipe ruptured in an underground installation in Duluth. Since the outage, experts deny that steam pipe damage was the cause but aren't supplying additional information.



Resident had local exchange telephone service however, all long distance access was lost. This meant that long distance, cell phone and internet service was not available during the twelve hour outage. The 911 service for the area was also lost due to the manner in which the emergency calls are handled. 911 Emergency calls are routed to Duluth where the caller's location is identified and the call routed to the correct emergency dispatch center. The cable failure broke the link to Duluth.

The solution to the loss of 911 service was to station volunteer firemen at fire stations who relayed emergency calls to Grand Marais. Amateur radio operators provided a link from the Grand Marais hospital to a medical center in Duluth.

The U.S. Border Patrol lost communications and improvised a multi radio relay set-up to communicate with their

Lake County Outage *cont'd on page 2*

The ARES COMMUNICATOR is published for the benefit of Amateur Radio Operators in Scott County and other interested individuals.

EDITOR: Bob Reid, Scott County Emergency Coordinator
Snail Mail: 13600 Princeton Circle
Savage, MN. 55378
E-Mail: N0BHC@aol.com
Phone: Home 952-894-5178 Portable 612-280-9328

Chile Quake

A massive 8.8 magnitude earthquake hit Chile at 0634 UTC on February 27, 2010, triggering a potential tsunami. IARU Region 2 and the Red Chilena Nor Austral de Servicio (RECNA) have suggested Amateur Radio operators monitor the following emergency communications frequencies for traffic pertaining to the earthquake and tsunami: 3.738, 3.750, 7.050, 7.100, 14.200, 14.350, 21.200, 21.350, 28.300 and 28.500 MHz.

IARU Region 2 Area Emergency Coordinator Jorge Sierra, LU1AS, reports that there is now traffic at frequencies of 40 meters from people seeking information from people in Chile: "We would appreciate if amateurs would leave free the frequencies used by RECNA, as well as the usual IARU Region 2 frequencies on in 20, 40, and 80 meters."

In addition to the above frequencies, you may also want to listen to the worldwide emergency communication Center of Activity frequencies: 14.300, 18.160 and 21.360 MHz. Other suggested monitoring frequencies are 3.720, 7.045 and 7.060 MHz. Hawaiian Amateur Radio operators on the lookout for a possible tsunami are monitoring 7.088 and 3.888 MHz.

BREAK - OVER

ARES Activities

Weekly Net Monday 7 PM 146.535 mhz (s)
Breakfast Saturday, March 13th
Digital Monday March 15th

SELECTED TRAFFIC NETS

Designator	Freq.	Local Times	
MN Phone	3.860Mhz	Noon, 5:30pm	Daily
MN CW	3.605Mhz	6:30pm, 9:50pm	Daily
ARES			
Scott ARES	146.535 S	7:00pm	Monday
Carver ARES	147.165+	8:30pm	Sunday
Bloomington	147.090+	9:00pm	Sunday
Neighboring Nets			
North Dakota	3.937Mhz	6:30pm	Daily
South Dakota	3.870Mhz	6:00pm	Daily
Wisconsin	3.985Mhz	5:30pm	Daily

Lake County Outage - *cont'd from page 1*

North Dakota regional headquarters. The Border Patrol officers also worked with the Canadian Border agents a couple steps across the border who had landline communications and also used satellite phones.

The interconnection of the communications systems apparently came as a surprise to emergency officials in the northeastern counties. Reports quoted officials as being surprised at the number of technologies that are connected to fiber optic cable, i.e.; cellular phones, internet, ATMs, etc.

One emergency response official intends to promote County personnel becoming ham radio operators and to begin working more closely with local ham radio operators.

BREAK - OVER

Daylight Savings Time

Spring Ahead
Sunday March 14th

Scott County ARES Contacts

Emergency Coordinator
Bob Reid N0BHC
13600 Princeton Circle
Savage, MN 55378
952-894-5178
N0BHC@arrl.net

Asst. Emergency Coordinator
Bob Minor W0NFE
5210 West 141st Street
Savage, MN 55378
952-894-2657
W0NFE@arrl.net

Asst Emergency Coordinator
Daniel Vande Vusse N0PI
5722 West 141st Street
Savage, MN 55378
952-440-1878
N0PI@arrl.net

Test Your NIMS Knowledge

ARES members are familiar with the Incident Command System from their study of the FEMA Institute courses. Now it is time to see how much you remember from those courses! Each month you will have the opportunity to test your ICS knowledge on a questions dealing with one ICS area.

This month we will take a look at some of the concepts from the IS-100 course, Introduction to Incident Command System. This is the first of the FEMA courses all ARES members must complete before participating in any response activities. You can find the course materials at this site: http://training.fema.gov/EMIWeb/IS/is100.asp. Now, test your knowledge of the ICS.

Here is the question for this month:

Which Command Staff position serves as the primary contact for supporting agencies assigned to an incident?
A. Safety Officer
B. Liaison Officer
C. Resource Officer
D. Public Information Officer

The answer will appear in next month's newsletter.

February Test Your NIMS Solution

Which General Staff position conducts tactical operations, develops the tactical objectives and organization, and directs all tactical resources?
B. Operations Section Chief

CORRECTION!

Last month the answer given for the January NIMS question was incorrect. The January question asked, "Which General Staff position prepares and documents the Incident Action Plan, collects and evaluates information, maintains resource status, and maintains documentation for incident records?"

These activities are right out of the position description for the Planning Section Chief, choice "A". Hopefully none of the Logistics Team members were shocked by the change in their responsibilities indicated by the incorrect answer!

BREAK - OVER

"Why not go out on a limb?
Isn't that where the fruit is?"
Mark Twain

Time to Upgrade ?

Spring is a great time to move up

If you are thinking about taking the plunge and upgrading your license, or becoming an amateur, there have never been more resources available. Many at no cost.

The pool of exam questions for the Technician Class entry level license has recently been revised. Study materials based on the new question pool are available.

The first step is to purchase a study guide for the license class you are targeting. You can find guides for all license classes at the ARRL bookstore (http://www.arrl.org/catalog/ - search on license manual). Once you get the study guide you can test your knowledge on several websites that offer practice exams. Some sites allow you to register, at no cost, and questions that you answer successfully are not included in future exams. This lets you narrow down the topics to target your study time.

Here is a list of some on-line exam sites. This is by no means a conclusive list but will give you a good sampling of the help available. Don't overlook another amateur as a source of information when concepts get confusing.

> QRZ.com Online tests for Technician, General, and Extra
http://www.qrz.com/p/testing.pl
> Radio Exam Online tests for Technician, General, Extra
http://www.radioexam.org/
> W8MHB US Amateur Radio Practice Exams
http://www.w8mhb.com/
> AA9PW FCC Exam Practice
http://aa9pw.com/
> Amateur Exam Study Program
http://www.n3fjp.com/tests.htm
> KB0MGA Practice Exams
http://kb0mga.net/exams/
> Ham test Online
http://www.hamtestonline.com/

BREAK - OVER

May your joys be as bright as the morning,
and your sorrows merely be shadows that fade in the sunlight of love.
May you have enough happiness to keep you sweet,
enough trials to keep you strong,
enough sorrow to keep you human,
enough hope to keep you happy

Digital Bulletins

W1AW to Alternate Digital Mode Schedule

Beginning Monday, March 15, 2010, W1AW will alternate the digital modes used for its digital bulletin transmissions.

While Baudot, PSK31 and MFSK16 still make up the digital mode complement, the schedule will be altered to give more exposure to PSK31 and MFSK16.

Because of time constraints and the varying lengths of digital bulletins, there were many instances where only Baudot was used. With the new schedule, amateurs preferring either PSK31 or MFSK16 will find these modes no longer secondary.

The regular callup will be made using the mode that is transmitted first. The digital bulletin times remain at 6 PM and 9 PM eastern, daily.

The new digital schedule is as follows:

Mon: Baudot, PSK31, MFSK16
Tue: PSK31, MFSK16, Baudot
Wed: MFSK16, Baudot, PSK31
Thu: Baudot, PSK31, MFSK16
Fri: PSK31, Baudot, MFSK16

The complete W1AW schedule can be found on page 100 of the January issue of QST, or on the web at, http://www.arrl.org/w1aw.html#w1awsked.

BREAK - OVER

Digital Contest Calendar

PODXS 070 Club

http://www.podxs070.com

EA (Spain) PSK31 Contest

Mar 13 1600Z – Mar 14 1600Z
Freq: 10M, 15M,20M,40M,80M Region1 band plan
Contest Call: "CQ EA TEST"
Single and Multi Op Classes
Exchange: EA Stns: RST + Province code
DX Stns: RST + QSO#
Scoring: 1 point per QSO, Mults: Province, Call areas
Complete Info: http://www.ure.es/contest/428-ea-psk31-contest-english-version.html

Haiti Medishare Operation

Amateurs + MARS + Ham Ingenuity = Success!

After the 7.0 magnitude earthquake struck the island nation of Haiti on January 12, many Amateur Radio operators asked how they could volunteer their time and service to assist with communications support. When Project Medishare — a partnership between the University of Miami Medical School (UM) and physicians and health officials in Haiti — needed help with their communications, Amateur Radio operators were quick to respond.

Medishare has constructed several health clinics in Haiti over the years — all of which were destroyed in the earthquake. "Medishare was able to rapidly deploy medical teams and assets to begin the overwhelming task facing the post earthquake medical needs," reported Jack Satterfield, W4GRJ/AFA4DG. "A field hospital was established within the relatively secure boundaries of the airport in Port-au-Prince. The overall conditions were basic to primitive; however, the medical care being provided was extremely high considering the overall conditions. We needed to establish sustainable logistics to support the hospital and the more than 100 volunteers who were rotating in and out every 5-7 days. Establishing reliable local and international communications was a high priority. UM, through its internal IT group, set up two broadband Vsat satellite links to handle e-mail and two channels of voice Voice over Internet Protocol (VoIP) phone circuits."

Satterfield said that the problem with the Vsat system was stability and reliability: "UoM Vice President for Facilities and Operations Ron Bogue was the Director in Charge of the Haiti operations. His concern about the unreliable communications caused him to contact Julio Ripoll, WD4R, with whom he has worked for years as the architect for UoM Medical facilities." Ripoll then contacted ARRL to request help in soliciting volunteers. ARRL immediately sent down an HF Go Kit — through the ARRL's Ham Aid Program — and put Ripoll in touch with ARRL Florida ARES leaders and Navy MARS Florida State Deputy Director Neil Lauritsen, W4NHL/NNN0TFH.

"Julio explained to Neil the mission profile and told him that he only had two WX4NHC operators ready to go to Haiti at that time, but that he had requested operators to go to Haiti to support two or three weeks of backup communications until such time the UoM is able to stabilize their permanent satellite system," Satterfield told the ARRL. "WX4NHC Coordinator John McHugh, K4AG, assembled the list of equipment and UM/Medishare provided an emergency purchase order and the equipment for both stations — one in Haiti and one in Miami — and we received the equipment the very next day."

Amateur Radio operators — some affiliated with WX4NHC, some with MARS — helped to provide communications support in Haiti. (ARRL Photo)

Simultaneous to the first Haiti Team being deployed, the WX4NHC Club built a complete station at the Haiti Command Center Building at UoM Medical Campus — even erecting antennas on the roof in two days.

The original mission profile was to set up a HF station capable of providing back up voice via phone patch and back-up e-mail capability via *Winlink*. According to Satterfield, both of these objectives could be met using normal Amateur Radio frequencies, but with limitations due to propagation and stations available when needed for phone patch traffic, the team decided to increase their flexibility and overall capability by using MARS assets "to extend the *Winlink* stations available and the Air Force MARS dedicated phone patch circuit that is available 24/7," Satterfield said. "The volunteer teams were arranged in teams of two operators, with at least one being a MARS operator. Since I was on Team 1, I had the opportunity to set the station up and establish basic operating procedures.

Satterfield told the ARRL. "We got the station operational for *Winlink* and phone patch traffic. The VHF was set on

Haiti Medshare Operation *cont'd on page 5*

Haiti Medcom Operaton - *cont'd from page 4*

146.52 for communications with Ron Tomo, KE2UK/AAT2BC, at the Nassau medical clinic, approximately 5 miles from our location. The Nassau medical clinic was very limited in medical resources; consequently, there was a lot of traffic between our respective stations using Miami Medical as a resource for patient consulting and patient transfers to Miami Medical, to other medical facilities and to the USNS *Comfort*, a hospital ship operated by the United States Navy."

Once the need to establish direct communications with the USNS *Comfort* was apparent, Satterfield said that the Amateur Radio communications support teams needed to get their VHF radio working on the marine frequencies: "We were able to download the MARS mod info for the FT-1900 and got it operational on the marine frequencies. Since I am a licensed USCG Captain (fishing guide), I am very familiar with the marine channels and protocol. We contacted the USNS *Comfort* on guard channel 16, using station ID as 'MARS RADIO Port-au-Prince Airport.' Once contact was made, we moved to working frequencies and passed the priority and emergency traffic. Communications with the USNS *Comfort* were conducted seamlessly by using MARS training of short messages with the strict use of PRO-WORDS. The communication link with the *Comfort* was critical to saving a lot of lives.

CARIBBEAN SEA The Military Sealift Command hospital ship USNS Comfort (T-AH 20), left, and the Military Sealift Command fleet replenishment oiler USNS Leroy Grumman (T-AO 195) conduct an underway replenishment in the Caribbean Sea. Comfort temporarily left Haiti to re-supply, but will return to continue supporting Operation Unified Response. (U.S. Navy photo)

Satterfield said the Amateur Radio teams were able to conduct approximately 25 phone patches on the Air Force phone patch net and the maritime 14.300 net. "Having access to the Air Force phone patch net was extremely valuable, providing virtually 100 percent phone patch availability, regardless of propagation or time of day or night," he told the ARRL. "All were routine health and welfare traffic, and were extremely appreciated by the Miami Medical personnel. We were also asked to establish a communications link with the US Joint Operations Command (JOC) to coordinate certain local security concerns. We were able to establish contact with JOC on 50.125 MHz. Again, strict use of MARS protocol, including use of PRO-WORDS, made for seamless communications."

"The major item that jumps out of this operation is the importance of *interoperability*," Satterfield told the ARRL. "I know a lot of our recent MARS training and exercises have been focused on interoperability, but this actual event put it to the ultimate test. The Army, Navy/Marine Corps and Air Force MARS each stepped in with a coordinated effort, and each with a defined support role. In addition, the ARRL was there from the beginning with equipment — through its Ham Aid Program — and reciprocal licensing support by contacting the FCC to clear the use of commercial traffic, to support of ordering medical supplies and other commercial logistic requirements." Lauritsen concurred: "The combination of available frequencies — both MARS and the amateur frequencies — as well as the combination of operators, allowed us to provide the best of both worlds in communications to the University of Miami and to Nassau University Medical team and to the Southern Baptists' SBDR group. All three non-governmental organizations have had nothing but praise for our volunteers."

The combined Amateur Radio/MARS efforts to support the University of Miami Project MEDISHARE ended on Monday March 1, 2010.

BREAK - OVER

Interoperability

The ICS213

ARES operators understand the importance of common procedures in emergency communications. We practice standard operating procedures and prowords in our training nets. We even use the same phonetic alphabet to limit the errors due to misunderstanding.

FEMA recognized these same principles regarding communications during an emergency response. The ICS uses a standard form to facilitate written communications for the same reasons amateurs use a particular message handling protocol. The goal is to reduce errors and increase speed.

FEMA labels this written form ICS213. The 213 is usually a two part carbonless form. You can find a copy of the form at: http://training.fema.gov/EMIWeb/IS/ICSResource/ICSResCntr_Forms.htm. The served agency will always specify the particular forms used during an emergency response.

Scott County Emergency Management will most likely be the served agency in any response for Scott County ARES. Scott County Emergency Management uses the form shown on the FEMA resources website.

Scott ARES uses a procedure to handle the ICS213 form that takes advantage of the knowledge and experience of ARES members and is transparent to the emergency responders.

ARES members are comfortable with the NTS formal traffic template. The same principles in the NTS format that promote accuracy and speed are applied to the ICS213. ARES members will feel comfortable with the procedure after a couple of practice runs. You can find the procedure on the Scott ARES website on the Member Resources page under Formal Traffic Handling. You will also find the ICS213 form in both PDF and MSWord files.

ARES members should download and review the procedure and print a couple copies of the forms for use as practice pages. The ICS213 form can be completed in notepad, saved as a text file, and sent via NBEMS in error correction mode. ARES ops should practice this process until they are comfortable with the procedure. The weekly training net provides an ideal place to work out any problems and answer any questions.

MARS Unifies Operation in Support of Haiti Relief Effort

To assist the MARS communications support effort in Haiti, the heads of the Army, Air Force, and Navy-Marine Corps MARS programs have agreed to divvy up responsibilities among the three Service MARS programs. According to Air Force MARS Public Information Officer David Trachtenberg, N4WWL/AFA3TR, this delegation of responsibility will facilitate more efficient utilization of MARS communications assets in the overall relief operation. On January 12, a 7.0 earthquake struck Haiti, killing thousands and wiped out the island nation's communication infrastructure.

Trachtenberg told the ARRL that Air Force MARS will have primary responsibility for coordinating and releasing public affairs information on the activities of MARS radio operators assisting with the Haiti relief operation. Navy-Marine Corps MARS will be responsible for recruiting volunteers — who will travel to Florida at their own expense — to serve in Haiti as part of the essential communications link. Army MARS will coordinate frequency authorizations and use of digital communications for MARS operations on the island, including the transmission of e-mail via radio links; this capability is especially useful in the absence of Internet connectivity.

"The delegation of responsibilities among the three MARS services not only makes practical sense, but is an excellent example of interoperability in action," said Air Force MARS Chief Allen Eiermann. "This represents true unity of effort," added Army MARS Chief. Navy-Marine Corps MARS Chief Bo Lindfors noted that the success of the MARS operation so far "demonstrates the value of this contingency communications capability in a real-world emergency."

According to Trachtenberg, volunteer MARS radio operators representing all three Service MARS programs have been on the ground in Haiti, working with military and medical teams to provide valuable communications support.

"The best index to a person's character is; How he treats people who can't do him any good, and; How he treats people who can't fight back."

Abigail Van Buren

Rootkit to blame for Windows Blue Screen of Death

Microsoft has confirmed that a rootkit caused Windows PCs to crash after users applied a security patch issued early in February.

Once a system had become infected with the Alureon rootkit it was trapped in the Blue Screen of Death (BSOD) problems that prevented booting. Microsoft investigators reported, "Our investigation has concluded that the reboot occurs because the system is infected with malware." The team concluded that the MS10-015 update was not at fault.

Microsoft's conclusion that malware was to blame was not unexpected. Shortly after the problem surfaced, researchers identified the rootkit, also called TDSS, Tidserv and TDL3, as the likely culprit.

Within hours of the release of MS10-015 and a slew of other security updates, users reported that their computers wouldn't restart. Microsoft halted automatic distribution of MS10-015 immediately and launched an investigation.

Microsoft sleuths reached the same conclusions as independent technicians who earlier had blamed an address conflict between MS10-015 and the rootkit for the debacle. The Malware writers had modified Windows behavior by attempting to access a specific memory location, instead of letting the operating system determine the address. When the upgrade, MS10-015, was downloaded and installed, the location of Windows code was changed. On the next reboot the malware code crashed attempting to call a specific address in Windows code which was no longer the intended OS function. MS10-015 patched a 17-year-old bug in all 32-bit versions of Windows.

Microsoft techs did not catch the conflict because it's difficult to create malware interaction tests with these types of infections which often leave the machine in such an unstable state that it cannot be reliably tested. Microsoft confirmed that all 32-bit versions of Windows were susceptible to Alureon-caused crashes, including Windows 7, even though the bulk of complaints came from users running Windows XP. That shouldn't be a surprise: XP is the dominant operating system worldwide.

Several security firms have published instructions and tools for users trapped with a BSOD, Microsoft recommendation for those users affected was to back up important files and completely restore the system from a cleanly formatted disk. If customers cannot confirm removal of the Alureon rootkit using their chosen anti-virus/anti-malware software, this is the most secure option.

cont'd col. 2

Spam Network Shut Down

A US judge granted a request to shut down 277 internet domains, which it said were used to "command and control" the so-called Waledac botnet.

A botnet is a network of infected computers under the control of hackers. Microsoft said that closing the domains would mean that up to 90,000 PCs would stop receiving orders to send out spam.

A recent analysis by the firm found that between December 3rd and 21st "approximately 651 million spam e-mails attributable to Waledac were directed to Hotmail accounts alone". It said it was one of the 10 largest botnets in the US. Machines in a botnet have usually been infected by a computer virus or worm. Typically, users do not know their machine has been hijacked.

Microsoft said that although it had effectively shut down the network, thousands of computers would still be infected with malware and advised people to run anti-virus software.

The court order was part of what was called "Operation b49". Along with intelligence organization Shadowserver, the University of Washington and security firm Symantec, Microsoft managed to get a court in Alexandria, Virginia, to force Verisign, which manages the .com domain, to temporarily switch off the domains.

Microsoft said it was the result of months of investigation and described it as a legal first. "This action has quickly and effectively cut off traffic to Waledac at the .com or domain registry level, severing the connection between the command and control centers of the botnet and most of its thousands of zombie computers around the world."

BREAK - OVER

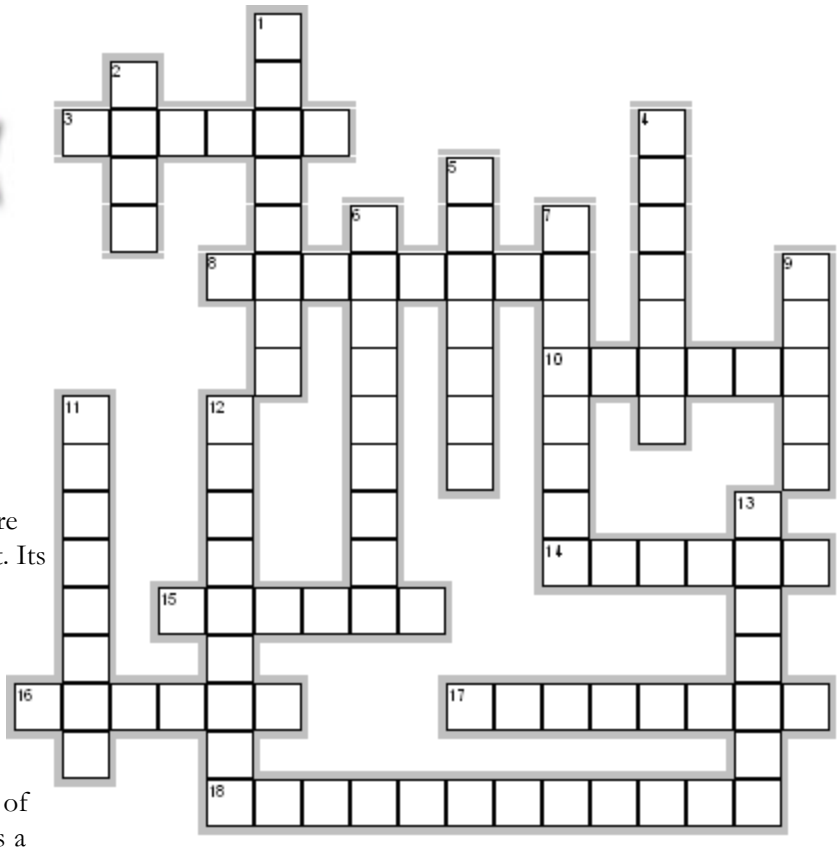
Rootkit *cont'd from col. 1*

Kaspersky Lab offers a less extreme workaround: a free utility that seeks out and destroys the rootkit. Symantec, meanwhile, has urged users to replace rootkit-infected drivers with clean copies.

Microsoft will provide a way for users to detect and remove the Alureon rootkit from infected PCs when they have the tool ready as part of their regular updates. In the past, Microsoft has used its Malicious Software Removal Tool (MSRT), a free program updated each Patch Tuesday, to seek out and destroy rootkits. The next scheduled refresh of the MSRT is March 9th.

BREAK - OVER

COMPUTER CREEPS



Across

3. Another name for a hijacked computer that is a member of a botnet.
8. Either a program or a feature built into hardware and which sits between a computer and the internet. Its job is to filter incoming and outbound traffic. Supposed to stop net-borne attacks such as worms reaching your PC.
10. Someone who steals or trades exclusively in stolen credit card numbers and their associated information.
14. Like the wooden horse of legend this is a type of program or message that looks benign but conceals a malicious payload.
15. Unwanted programs that, once installed, bombard users with unwanted adverts. Sometimes pose as fake computer security software.
16. A large number of hijacked computers under the remote control of a single person via net-based command and control system.
17. A hacker that uses his or her skills for positive ends and often to thwart malicious hackers.
18. An unskilled hacker who originates nothing but simply steals code, techniques and attack methods from others.

Down

1. The practice of sending out e-mail messages that look as if they come from a financial institution and which seek to trick people into handing over confidential details.
2. Self-propelled malicious program that scours the web seeking new victims - in the past this has been used to distinguish it from a virus that requires user action to compromise a machine.
4. Malicious program that, once installed on a target machine, steals personal and confidential information. Distinct from adware.
5. A virtual "room" on the IRC text chat system. Most are usually dedicated to a single topic.
6. Program installed on a victim's machine that records every keystroke that a user makes. These tools can obviously be very useful for stealing login and password details.
7. A hacker that uses his or her skills for explicitly criminal or malicious ends. Has been used to mean the writers of destructive viruses or those that use attacks to knock websites offline.
9. A malicious program - usually one that requires action to successfully infect a victim. For instance - the malicious programs inside e-mail attachments usually only strike if you open them.
11. An individual computer or a network of machines set up to look like a poorly protected system but which records every attempt, successful or otherwise, to compromise it.
12. The numerical identifier that every machine attached to the internet needs to ensure the data it requests returns to the right place.
13. A term for all malicious software covers any unwanted program that makes its way on to a computer.

May the sun shine all day long, everything go right and nothing wrong. May those you love bring love back to you, and may all the wishes you wish come true!

MEDAL OF HONOR DAY

March 25, 2010

Gov. Pawlenty signed a bill designating March 25th as Medal of Honor day in honor of Minnesotans who have served in the military or naval forces of the United States and received the Congressional Medal of Honor, which was first presented on March 25, 1863.

The first formal system for rewarding acts of individual gallantry by the nation's fighting men was established by General George Washington on August 7, 1782. Designed to recognize "any singularly meritorious action," the award consisted of a purple cloth heart. Records show that only three persons received the ward: Sergeant Elijah Churchill, Sergeant William Brown, and Sergeant Daniel Bissel Jr.

The Badge of Military Merit, as it was called, fell into oblivion until 1932, when General Douglas MacArthur, then Army Chief of Staff, pressed for its revival. Officially reinstituted on February 22, 1932, the now familiar Purple Heart was at first an Army award, given to those who had been wounded in World War I or who possessed a Meritorious Service Citation Certificate. In 1943, the order was amended to include personnel of the Navy, Marine Corps, and Coast Guard. Coverage was eventually extended to include all services and "any civilian national" wounded while serving with the Armed Forces.

Although the Badge of Military Merit fell into disuse after the Revolutionary War, the idea of a decoration for individual gallantry remained through the early 1800s. In 1847, after the outbreak of the Mexican-American War, a "certificate of merit" was established for any soldier who distinguished himself in action. No medal went with the honor. After the Mexican-American War, the award was discontinued, which meant there was no military award with which to recognize the nation's fighting men.

Early in the Civil War, a medal for individual valor was proposed to General-in-Chief of the Army Winfield Scott. But Scott felt medals smacked of European affectation and killed the idea.

The medal found support in the Navy, however, where it

cont'd col. 2

Tech Questions Released

Revised exam questions published

In January, the Question Pool Committee (QPC) of the National Conference of Volunteer Examiner Coordinators (NCVEC) released the 2010 Technician (Element 2) Question Pool. Upon further review of the pool, members of the QPC found and corrected more than 50 minor typographical errors and clarified the questions and answers, making them easier to understand.

These adopted changes are now incorporated in a revised question pool. The errata list, as well as the revised Technician question pool, is available on the NCVEC Web site at, http://www.ncvec.org/.

The previously released pool dated January 4, 2010 is invalid for use. The newly revised Technician question pool will become effective for all examinations administered on or after July 1, 2010; it will remain valid until June 30, 2014.

The current Technician question pool that became effective July 1, 2006 will expire June 30, 2010. The new Technician pool contains approximately 400 questions, from which 35 are selected for an Element 2 examination; it will contain graphics and diagrams, something new for this element.

The current General class question pool was effective July 1, 2007 and is valid through June 30, 2011. The current Amateur Extra class pool was effective July 1, 2008 and is valid until June 30, 2012.

BREAK - OVER

Medal of Honor *cont'd from col. 1*

was felt recognition of courage in strife was needed. Public Resolution 82, containing a provision for a Navy medal of valor, was signed into law by President Abraham Lincoln on December 21, 1861. The medal was "to be bestowed upon such petty officers, seamen, landsmen, and Marines as shall most distinguish themselves by their gallantry and other seamanlike qualities during the present war."

Shortly after this, a resolution similar in wording was introduced on behalf of the Army. Signed into law July 12, 1862, the measure provided for awarding a medal of honor "to such noncommissioned officers and privates as shall most distinguish themselves by their gallantry in action, and other soldierlike qualities, during the present insurrection."

Although it was created for the Civil War, Congress made the Medal of Honor a permanent decoration in 1863.

Almost 3,400 men and one woman have received the award for heroic actions in the nation's battles since that time.

BREAK - OVER

Wireless Capacity Shrinking

Wireless Operators Facing Data Capacity Issues

A scramble for network capacity to accommodate the explosive growth in mobile data traffic was a common theme at this year's Mobile World Congress in Barcelona, Spain. Many wireless network operators are struggling to manage network congestion as they seek to profitably harness the added traffic driven by a boom in mobile Internet usage.

In many cases, data revenues for these network operators are growing slowly at best despite the added usage, making effective data traffic management a high priority. Research firm Informa that forecasts a 50 percent rise in mobile data traffic in 2010, driven in large part by the increasing popularity of devices such as Apple Inc.'s iPhone and netbooks. However, during the same time the industry saw only a 13 percent increase in data revenues.

The problem has intensified pressure on network operators to find ways of using fixed line networks, such as the Internet, to relieve some of the burden from wireless network facilities. "Offloading is crucial for us," said Olaf Swantee, who leads mobile operations for France Telecom-owned Orange. "In many countries where we have a fixed network we try to offload directly," he added.

The challenge is that shifting data from wireless networks to local hotspots costs money, and operators are scrambling for solutions that will not raise their overall capital spending, according to industry executives. "To address the smartphone challenge they are investing again," Rajeev Suri, CEO of Nokia Siemens, told Reuters.

It is not certain whether these investments are supplementing or replacing other investments, he said.

But Bruce Brda, head of rival Motorola's networks business, was clear that network operators are not increasing their spending. "Carriers have been very consistent — they do not increase capex," he told Reuters.

However, Motorola saw higher than expected equipment demand late last year as some network operators bolstered their existing networks to manage additional data traffic, Brda added. "In early 2010 I am seeing the same trend. The indication is there is incremental spending," he said.

Network equipment suppliers such as Nokia Siemens, Ericsson and Alcatel-Lucent also demonstrated their new LTE (Long Term Evolution) equipment in Barcelona, which provides operators a step toward managing additional wireless data traffic.

Operators are expected to spend billions converting their networks to the LTE standard, which enables high-speed mobile broadband access for services such as viewing movies on mobile devices.

But some critics say the new standard offers only a temporary solution should wireless data traffic continue its current growth trajectory. "LTE will buy a carrier two to three years of relief, but then it runs out," Brda said.

Some analysts say that network operators' sales in more mature markets are not growing fast enough to justify significant investments, which could spur demand for alternate technologies such as Wi-Fi or femtocells.

Femtocells are localized phone network base stations that reside in homes and offices where traditional wireless signals might be weak. The traffic is then taken onto the telecom company's network via the customer's broadband Internet connections. "The biggest problem is that everybody is expecting these huge amounts of data but nobody is willing to pay much extra for it," Stephen Rayment, chief technology officer of Belair Networks, which provides Wi-Fi services. "Operators started offering 'all you can eat' data and now that's coming back to bite them."

cont'd col. 2

BREAK - OVER

February Crossword Solution

Across

3. RHYMES—Something a poet writes.
6. RING—Something you wear on your finger.
8. LOVE—A Valentine's Day emotion.
9. CARDS—People often exchange these on Valentine's Day.
10. HEART—The symbol of love.
12. ROSE—The flower of love.
14. DATE—Go on a _____ (with your sweetie)
15. CHOCOLATES—A Valentine's Day treat.
16. CANDY—A Valentine's Day treat.
17. ILOVEYOU—Something often written on Valentine's Day cards.

Down

1. ARROWS—What cupid shoots.
2. VERSE—Something a poet writes.
4. GIFT—Present.
5. KISS—Touch lips.
7. VALENTINESDAY—A day for love.
11. RED—Valentine's Day color.
13. FEBRUARY—The month of Valentine's Day
15. CUPID—He shoots love arrows.

Kneber botnet

Virus attacks 75,000 computers worldwide

A new computer virus has infected almost 75,000 computers worldwide - including 10 U.S. government agencies - collecting login credentials from online financial, social networking sites and email systems and reporting back to hackers.

The virus, dubbed the Kneber botnet, is thought to be the brainchild of an Eastern European criminal group that is likely selling the information on the black market, according to the Internet security firm NetWitness, which uncovered the attacks in January. The FBI, Department of State and Department of Homeland Security are investigating. The crime groups "running this activity are every bit as expert at compromising systems and siphoning off information as nation states," say the virus experts.

"They're well funded, motivated and successful." Hackers using the new virus have infiltrated the computer networks of more than 2,400 companies in almost 200 countries over an 18-month period, NetWitness, the Herndon, Va.-based computer security firm reported. Further investigation revealed that many commercial and government systems were compromised, including 68,000 corporate login credentials and access to email systems, online banking sites, Yahoo, Hotmail and social networks such as Facebook.

Infiltrated companies include pharmaceutical giant Merck & Co., Cardinal Health Inc., software firm Juniper Networks and Paramount Pictures, according to the Wall Street Journal. Companies in Egypt, Mexico, Saudi Arabia, Turkey and the U.S. are the most frequently targeted in the attack, according to a research paper released by NetWitness.

The attack uses a piece of software called ZeuS, designed in Eastern Europe, that takes control of large numbers of computers. ZeuS is among the top five most reported computer infections, according to the Department of Homeland Security.

"These large-scale compromises of enterprise networks have reached epidemic levels," said Amit Yoran, CEO of NetWitness and former Director of the National Cyber Security Division. "Cyber criminal elements like the Kneber crew quietly and diligently target and compromise thousands of government and commercial organizations across the globe." Yoran said that conventional intrusion detection systems are "inadequate for addressing Kneber or most other advanced threats."

BREAK - OVER

Quick Training Tips

Emergency Nets

A smoothly operating net is key to providing accurate rapid communications for our served agency. Over the next several months we will be reviewing some basic principles of emergency net operations that are part of an efficient net. Many of the items we review will seem obvious and some strange but all are designed to accomplish our goal.

Let's start out by describing a couple types of emergency nets. Open Net Format, or Informal Net: This type of emergency net may not be obvious. An example would be the group that appears on the designated Skywarn frequencies on afternoons with storm potential. The group is a result of self-activation of hams who are watching the local weather. There is a NECOS in the background who will relay any developing conditions to the NWS. Normal conversation between the stations keeps rotating informally among the stations on frequency.

Directed Net Format: There are two basic types of directed nets: Formal and Informal. One example of an informal directed net would be a radio club net. The informal directed net has a NECOS station providing general order and following an agenda that is know to the stations participating in the net.

The formal directed net is, as the name implies, a more rigid operation. The NECOS maintains strict control of the net activities by controlling check-ins and routing traffic. All communications take place under the guidance of the NECOS. Stations pay particular attention to basic operating procedures i.e.; prowords, ITU phonetics, traffic handling procedures, etc. The NECOS may set specific conditions for check-ins. All normal chatter stops when a directed net is activated.

ARES Breakfast
Saturday March 13th
7:30AM
Perkins Restaurant
Savage, MN

NECOS Schedule March 2010

1 Mar KC0YHH Tony
8 Mar N0PI Dan
15 Mar W0NFE Bob
22 Mar KB0FH Bob
29 Mar KC0YHH Tony
5 Apr N0PI Dan