

### **Commissioner's Cache**

The school year is upon us, and all of us here at CyberPatriot hope you had a wonderful vacation.

As you begin classes and form your teams, the CyberPatriot Program Office will begin its preparation for the competition season. First, we have a

CyberPatriot V "Sneak Preview" planned for September 8<sup>th</sup>. During the three-hour preview, registered teams will have the opportunity to test-drive the new CyberPatriot Competition System (CCS) and provide feedback on their experiences. Coaches and mentors have the sign-up information.

The competition season begins with the CyberPatriot Practice Round during October 1-12. If you are new to CyberPatriot or a seasoned veteran, we have new training materials for you on our website. The training modules were tailored for CyberPatriot V by one of our founding partners, the Center for Infrastructure Assurance and Security.

Coach registration ends on September 30, 2012, and the deadline for registering team members is October 26, 2012. We are well ahead of last year's record number of 1,019 registered teams. This year, 746 teams have registered as of this printing.

Good luck to you as you form your teams and train for CyberPatriot V. It promises to be a fun and challenging competition. As always, if you need any assistance, please contact the CyberPatriot Program Office at: info@uscyberpatriot.org.

Bernard K. Skoch Commissioner CyberPatriot Program

### Apples to Apples, Androids to Androids: New Vulnerabilities Come to Light

By Alison Fang Yuen, Assistant Editor

Like they're following the old adage, "Why buy the cow when you can get the milk for free?" some users do not pay for in-app purchases on their Apple iPhones due to a hack in the app store.

How the hack works is: First, the user installs fake certifications on his/her phone before following a few steps to connect to a special DNS (Domain Name System) server. When the user sends a receipt to the app store server to make an in-app purchase, it is redi- Brodeur of Leviathan Security rerected to a server controlled by the searched this vulnerability when hacker. The server responds as though the receipt is valid and the in-app purchases are free. According to MacWorld.co.uk, "For now there is no fix. Apple

simply promises that the

vulnerability will be addressed in iOS 6." However, the article gives suggestions on how app developers can address the vulnerability themselves. To read the article, click here.

The iPhone is not the only smartphone with new app vulnerabilities coming to light. Google's app restrictions are much less rigid than Apple's and criminals are taking advantage of it to steal user data. According to BGR.com, Paul he "created a special Android application that explores what data can be harvested" and "his application was able to access the SD

card, various system information and unique handset identification data." The scary part is that Brodeur's app had no permission from the user to gather any data. To read about Brodeur's findings, <u>click here.</u>

A vulnerability in the Android Beam (the Near Field Communication (NFC) that allows data transfer between two phones) has the default Beam setting set to open all files and to go to all Web links that are sent to it. A hacker using NFC can send a Web link to the phone, with a website running codes to exploit the known vulnerabilities of the phone. Then the hacker can view data (Continued on Page 4)

### **Program Office Bits**

**Congratulations to** Spokane Public Schools —

### the newest CyberPatriot Center of Excellence!

- Coaches' Online Meetings: Sept. 11 and 12, 2012
- Coaches' registration ends Sept. 30, 2012
- Students must be entered into the team websites by Oct. 26.2012
- Team registration payments are due Oct. 31, 2012
- Competition dates for CyberPatriot V can be downloaded at: http://www.uscyberpatriot.org/CP5/CP%20V% 20Documents/CPV Competition Sked.pdf



Team Wolfpack, from Civil Air Patrol's Colorado Springs Cadet Squadron, competing at the CyberPatriot IV National Finals Competition. The team was invited to Cyber Conference in Colorado Springs, due to their 1st Place finish in the CyberPatriot IV All Service Division. (See Page 3.)

### **This Month's** Question

What is vishing?

(The answer appears on Page 4.)

### **Features**

Page

- 1 Apples to Apples, Androids to Androids: New Vulnerabilities Come to Light
- 2 Sponsor Profile: Northrop Grumman
- 2 Time-Outs, Poems, and Games: A Short History of Viruses
- Spotlight on Colorado Springs 3
- Summer Camp Goes to 4 Cyberspace: Northrop Grumman Hosts First Ever Cybersecurity Summer Camp

 Air Force Association / CyberPatriot Program • 1501 Lee Hwy Arlington, VA 22209 • www.uscyberpatriot.org •

Publisher

Editor Francis S. Zaborowski

### **The CyberSentinel**

**Assistant Editor** 

Alison A. Fang Yuen

2

**CyberPatriot Program Office** •1501 Lee Hwy Arlington, VA 22209 • <u>www.uscyberpatriot.org</u> •E-mail: info@uscyberpatriot.org • Telephone: 877.885.5716

screen. To use the computer, the user would puter virus as a computer program within an have to reboot it. Elk Cloner was spread by floppy disks and would copy itself onto the computers. When the computer was re-While today's viruses are spread via the Interstarted, the virus just continued counting. To net in days, before the Internet, viruses were read more about the Elk Cloner, click here. spread by tapes or even floppy disks in weeks Brain (1986). First marketing virus and the

first root kit, created to stop pirating on IBM PCs. According to textfiles.com, the two brothers who developed the virus "wrote [it] so that it would infect machines running boot-

program to run a poem on Apple II computers.

Every fiftieth time the infected computer

started up, a poem would display on the

leg copies of a program [they were] selling for physicians. The original Brain put a copyright notice in the directory of the [5 ¼"] floppy disks, but did no other damage." However, the two messages that appeared on the screen concerned computer users. To read more about Brain and the different versions from textfiles.com, click here. The vaccination for this virus was to enter a signature into the correct place on the boot sector as the virus looked for that signature first. To read more about Brain, click here.

In short, PERVADE automatically downloaded a game, Elk Cloner would show a poem every fiftieth start-up, and Brain slowed down access to the diskette and caused time-outs. All were nuisances by today's standards. Just like a real virus, computer viruses have adapted and mutated into something far more destructive. Some notable offspring that followed were Jerusalem, the that were created and some have more than one name or version. However, all were malicious

Morris Worm, the Concept Virus, Happy99, Melissa, the Love Bug, MyDoom, Samy, Zeus, and Flame. These are only a few of the viruses

and some have versions still around today.

### Northrop Grumman Foundation President Sandra Evers-Manly presents a \$54,000 CyberPatriot scholarship check to AFA Chairman of the Board Sandy Schlitt at the CyberPatriot IV National Finals Competition. **Time-Outs, Poems, and Games: A Short History of Viruses**

# Sponsor Profile: Northrop Grumman

Northrop Grumman is a leading global security company providing innovative systems, products and solutions in aerospace, electronics, information systems, and technical services to government and commercial customers worldwide. Headquartered in Falls Church, Virginia, the company's core competencies are aligned with the needs of its customers and address emerging global security challenges in areas such as unmanned systems, cybersecurity, C4ISR, and logistics, all of which are critical to the defense of the nation and its allies. The company has more than 70,000 active employees, worldwide.

At Northrop Grumman, corporate responsibility is include Eco Classroom, CyberPatriot, VEX Roa key component of our business and operating strategies. We are committed to the advancement of science, technology, engineering and math (STEM) education and partner with organi-

Personal computers have been in use since

1977, and computer viruses have been around

nearly as long. The dictionary defines a com-

innocent-looking program that copies itself

and generally executes a malicious action.

to years. Three predecessors for today's vi-

ruses broke ground for the modern Trojans,

PERVADE (1975). First wild Trojan and consid-

ered the very first computer virus. Created by

writer John Walker, it was developed to auto-

game where the computer guesses the animal

matically distribute his ANIMAL program (a

the user is thinking of by asking yes-or-no

questions) onto Universal Automatic Com-

puters (UNIVAC). Spread by tapes, PERVADE

would copy itself to the directory whenever

ANIMAL was run. Walker wrote, in a letter to

the editor of Computer Recreations, "Within a

month or so, ANIMAL was well-established at

numerous installations of Univac computers."

Elk Cloner (1980). First widely spread PC virus

from outside the lab. Rick Skrenta wrote the

To read more about PERVADE, click here.

root kits, and large-scale virus outbreaks.

zations that provide unique programming to inspire the next generation of scientists, engi- more information. neers and technicians.

NORTHROP GRUMMAN

Northrop Grumman Foundation supports diverse and sustainable national-level programs that enhance the education experience for students and provide teachers with the training and tools they need to be successful in the classroom. The Foundation initiatives botics, Sally Ride Science, U.S. Space Camp, Science Buddies, Great Minds in STEM and the Virginia Initiative for Science Teaching and Achievement. Please visit

www.northropgrumman.com/foundation for









### **Spotlight on Colorado Springs**



### Team Wolfpack Stalks a Cyber Future at Colorado Springs

By Bill Blatchley, Colorado Springs Cadet Squadron Leader and Team Wolfpack Coach

*Colorado Springs* — The CyberPatriot IV All Service Division National Champions, Team Wolfpack of the Colorado Springs Civil Air Patrol, attended the Cyber 1.2 Conference held at the 28<sup>th</sup> National Space Symposium.

The team was invited to attend the conference due to their CyberPatriot performance. The Cyber 1.2 Conference started the 28<sup>th</sup> National Space Symposium on April 16, 2012. The symposium is presented annually by the Space Foundation to bring "together space leaders from around the world to discuss, address, and dream about the future of space." A cyberspace pre-symposium component was added in 2010 due to the fusion of cyberspace and aerospace.

Through the conference, the CyberPatriot team members learned of great career opportunities in cybersecurity. Each cadet came away with an appreciation of the education and training involved in becoming a cyber professional, be it in the military, government or private industry.

The conference opened with a speech by Lt. Gen. Michael Basla, Vice Commander, Air Force Space Command. Lieutenant General Basla stated, "Cyberspace is part of every fight we are in." Of particular interest to the CyberPatriot team, was information presented by Lieutenant General Basla on the cyberspace career development program being put in place by the Air Force. The program has instituted three levels of certification and has 5,700 officers, enlisted, and civilian personnel certified.

The general stated that airmen are always aware of the potential for FOD (foreign object damage) on the flight line. Airmen are constantly looking for items on the taxiway that might damage an aircraft. Meanwhile, the airmen of the 24<sup>th</sup> Air Force are looking for "FOD" that can damage their computers since unauthorized downloads or entering bad Web sites can do more damage than junk on a runway.

The cadets learned that the 24th Air Force has hunter teams looking for problems within the networks. The hunter teams participate in Red Flag exercises designed to simulate real world cyber encounters. The commander of the 24<sup>th</sup> Air Force, Maj. Gen. Suzanne Vautrinot, spoke of the operational side of the cyber mission. She stated the mission focus is based on orders just like air, sea, and land war fighters. The hunter teams find threats and neutralize them. They are focused on operations where the threat is highest. Major General Vautrinot had presented the awards to Team Wolfpack at the CyberPatriot Awards Ceremony of the National Finals.

Many CyberPatriot corporate sponsors were present in the vendor exhibit hall. During the symposium student tour, the members of the Colorado Springs CyberPatriot team visited the booths of CyberPatriot sponsors. The team thanked those sponsors for participating in the CyberPatriot program. Most had their space related divisions present for the Space Symposium. Those not exposed to CyberPatriot were interested in knowing how their respective companies were supporting high school students. However, every sponsor was interested in each team member's plan for the future and congratulated the team on their accomplishment.

As the team members talked with sponsors and other exhibitors, they gained further knowledge of the career opportunities available in the cyber world. Left: The CyberPatriot team poses with Lt. Gen. Michael Basla at the Space Symposium Cyber 1.2 lunch: (left to right) C/SrA. Christopher Ottesen; C/ Capt. Thomas Jessop; C/2dLt. Carlin Idle; C/CMSgt. Chris Vasquez; Lt. Gen. Basla, USAF; Capt. Bill Blatchley, CAP; SM. John Parish; C/AB. Stephen Parish; C/CMSgt. Amanda Church Photo credit, Space Foundation. Courtesy of Capt. Blatchley

CULL ALL OPTIROL





Above: Team Wolfpack cadets learn about satellite communications from a General Dynamics exhibitor: (left to right) Robert Rudolph, General Dynamics; C/CMSgt. Chris Vasquez; C/SrA. Christopher Ottesen; C/AB. Stephen Parish; C/2dLt. Carlin Idle; Capt. Bill Blatchley, CAP. Photo credit, Space Foundation. Courtesy of Captain Blatchley





Team Wolfpack of Colorado Springs, Civil Air Patrol won CyberPatriot IV's National Finals Competition, All Service Division. This photo was taken during the CyberPatriot IV Awards Ceremony.

### **Answer to Monthly Question**

The answer is: Vishing is phishing over voice networks. Criminals call victims and use social engineering to obtain personally identifiable information. Landlines, cell phones, and Voice over Internet Protocol (VoIP) services are vulnerable to vishing, due to the ability of criminals to spoof (fake) caller ID and interactive voice functions. For example: A victim receives a bogus automated call and the caller ID displays the name of a real credit card company with the criminal's telephone number. An interactive recording asks for a credit card number after a couple of innocent prompts. The scam is complete when the victim enters a credit card number. For more on vishing, see <a href="https://www.usaa.com/inet/pages/advice\_12\_common\_scams?">https://www.usaa.com/inet/pages/advice\_12\_common\_scams?</a>

### Summer Camp Goes to Cyberspace: **Northrop Grumman Hosts First Ever** Cybersecurity Summer Camp

Northrop Grumman and Chantilly Academy, a newly designated Governor's STEM School in Fairfax, Va., sponsored their inaugural Cybersecurity Summer Camp, August 7 - 10. The goal of the camp was to excite and educate the next generation of cyber professionals to fill the critical gap in our nation's cyber workforce.

Seventy Fairfax County Public High School students in grades 9-12 with both intermediate and beginner-level knowledge of computers, networks and cybersecurity enrolled in the camp, which was held at Chantilly High School. The curriculum was based on the highly successful CyberPatriot program and included demonstrations and lab exercises taught by instructors from the Northrop Grumman Cyber Academy and CyberPatriot mentors. These instructors educated students about cybersecurity fundamentals and managed the camp's grand challenge, like a mini-CyberPatriot competition, on the final day.

"The camp is another testament to Northrop Grumman's commitment to promote STEM and build the cyber workforce of tomorrow," said Diane Miller, director of operations, Northrop Grumman Cybersecurity Group. "Through this effort and initiatives like CyberPatriot, we can reach students early-on to inspire them to pursue a career in this field and help position them for success."

Northrop Grumman cyber experts served as guest speakers, highlighting the national challenges this field offers and providing advice about careers/internships at the company. Other speakers included Virginia Secretary of Technology Jim Duffey, who discussed cyber-related academic and career opportunities in Virginia, and Dr. Sushil Jojodia, Director of the Center for Information Security at George Mason University in Fairfax. Dr. Jojodia discussed college opportunities focused on security and gave demonstrations on threats for wireless and cell phone technologies.



Northrop Grumman employees mentor students at the Fairfax County, VA, Cybersecurity Camp.



## of the CyberPatriot Competitor Code of Conduct.

Apples to Apples,

(Continued from Page 1)

Androids to Androids (Cont'd)

on the phone. Click here for the Android Beam article.

In summary, there is a hack in the app store that enables

users to steal revenue from the app developers, Android

apps are able to download user data from phones, and a

hacker can exploit the NFC to view user data on the An-

droid. The app store hack enables users to commit piracy

and the Android issues involve hacking - also violations

To protect yourself, here are a few suggestions: For the Android apps, be careful as to what information is on your phone (credit card, bank accounts, social security number, etc.). Lastly, to protect yourself from the NFC exploitation, change the settings on the Android Beam so that your phone doesn't visit a website without your permission. By becoming more aware of the vulnerabilities in everyday devices, you can defend against hackers.

#### **Coaches' Corner**

- CyberPatriot V Coach Registration. CyberPatriot V Coach Registration is open at: www.uscyberpatriot.org. Coaches must be registered and cleared before their teams may register.
- Coaches' Online Meetings will be held in three 45minute repeat sessions on September 11 and 12 at different times to accommodate the different time zones and work schedules. Check your e-mail in September for details. To access the Coaches' meeting slides <u>click here</u> or go to <u>http://</u> www.uscyberpatriot.org/CP5/CP% 20V% 20Documents/Forms/AllItems.aspx
- CyberPatriot V Sneak Preview September 8, 2012 --12 noon –3 pm EDT. Try out the new CyberPatriot Competition System (CCS) online. The event is open to all registered coaches, mentors, and their teams. Contact info@uscyberpatriot.org if you are a registered coach and did not receive a participation survey.

### Staff Change

Our Assistant Editor, Alison Fang Yuen, ended her summer internship at the CyberPatriot Program Office on Tuesday, August 14, 2012. She is missed by the staff and others who served with her. The work she performed for The CyberSentinel and the Program Office was added value and her contributions will continue to have an impact the CyberPatriot Program. Hopefully, she will join us again. Good luck, Ali!

### Presenting Sponsor: ORTHROP GRUMMAN





**Founding Partners:** 

111111





### **Cvber Silver:**