NETWORKING 101

WEST VIRGINIA NETWORK (WVNET)

West Virginia Statewide Technology Conference 2016 (WVSTC 2016) will be held on July 19-21, 2016, at The Waterfront Hotel and the Morgantown Event Center in Morgantown, WV. It's not too late to **register**! "Innovate. Empower. Impact the World through STEM" is the theme of this year's conference. WVSTC 2016 will start with the opening of the Exhibitor Hall at 11:30am on Tuesday, July 19, followed by lunch at 11:50am. Immediately following lunch, conference participants will move upstairs for the opening keynote event. Judge Dan O'Hanlon, Director of WVNET, will offer opening remarks and introduce the opening keynote speaker.

Opening keynote speaker on Tuesday, July 19th at 1:00pm, is **Kelly Reddin, Global Master Trainer, Lego Education**, who is helping innovate education through the use of creativity. Closing keynote and awards luncheon will begin with West Virginia Department of Education's Chief Technology Officer, Mr. Sterling Beane. Closing keynote speaker on Thursday, July 21st at 11:00am, is **Brent Frey, Apple, Inc.**, who will share ideas on how to leverage technology as a change agent. WVSTC 2016 offers participants 131 concurrent sessions, 68 exhibiting vendors, 450 attendees and 1 STEM Playground. Join us on Tuesday from 5:15-7:00pm for STEM Playground with keynote exhibitors LEGO and Apple, and other exhibiting vendors as we go hands-on with all the new gizmos and gadgets. More conference info here: **www.wvstc.com**

Engaged: Hands + Brain = Creativity + Learning

Opening Keynote—Tuesday, July 19th—1:00PM

This keynote will be hands-on and minds-on! You will learn how being creative gets your brain engaged in learning. Using creativity makes teaching and learning more effective, more enjoyable, and more memorable. Come experience putting your hands to work in order to put your brains to work. **Read Bio**

Catch up, Keep up, or Lead — Brent Frey, Apple, Inc.

Closing Keynote—Thursday, July 21st—11:00AM

You have come to this conference because you're excited about the possibilities of technology for learning. Will you take back your new found knowledge and have an impact on other educators? How will what you've learned change your teaching practice? Are you able to inspire your colleagues? Can you turn your passion for technology in education into actions that will impact your community? Your leadership can make a difference on whether your school is catching up, keeping up, or leading. **Read Bio**

Technology Integration Specialists (75 attendees) will travel to Coopers Rock for an offsite field trip as a pre-conference session with Apple. The Coopers Rock Professional Learning Expedition provides the opportunity to learn new skills related to instructional practice, technology integration, and professional development planning and delivery. Modeled on the work done by the Harvard Graduate School of Education and Outward Bound USA, participants will be working at locations around Coopers Rock State Park, conducting experiments, creating materials and exploring aspects of the park through activities, grounded in WV curriculum standards, that promote student engagement, the use of technology and STEM focused instruction.

(Guest feature article by WVNET staff member Fran Barnes)

VOLUME 6, ISSUE 7

JULY 2016

PROTECTING STUDENT DATA

Employees who handle student records must make every attempt to protect the information, also known as PII (personally identifiable information). PII basically consists of any data that can identify a specific individual. Most of us would recognize the top-protected items as name, social security number, and birth date but there are more data items that can single out a person from a group. We must also protect names of parents, siblings, addresses, student id, biometric record (fingerprints, signature), place of birth, mother's maiden name, and other information that could be used to identify the student (work study assignment if only one person is employed at that location, for example).

We probably do things daily that risk this information getting into the wrong hands or that might allow another person to access PII. Even worse, we as employees do things that might allow another person to get into our database and damage records and we have an obligation to not allow this to happen. If this happens, you have a system breach. Here are a few simple things that each of us can do to help prevent a breach.

- Place your computer monitor in a position where it can't easily be read by people passing by your door or window, or seen by visitors to your office.
- Before you leave your desk unattended for more than a quick trip to the copier, log off of any applications that access PII or lock your screen (hold the Window key and tap the letter L).
- Don't allow another person to access a database using your account. NEVER share accounts.
- Protect your passwords. If you must write them down, keep them safe and secret. Don't write them on the calendar on your desk or keep them in a binder marked "Passwords".
- Don't print it if you don't need to. If you must print lists or documents with PII on them, don't leave them on your desk. They should be locked in a cabinet or desk drawer if you aren't using them and shredded as soon as they are no longer current.
- Protect 'end points' – laptop, USB drives, smartphones, printers, etc. Use portable storage like USB drives as little as possible.
- Maintain files on your computer or server only as long as you need them. Delete them as soon as you can.
- Don't leave documents on a printer.
- Think before you post/send/tweet information.
- Collect only what you need. For example, could you settle for the number of students in a given major rather than a list of names and id's?
- Distribute information only to those with a need to see it and only include the minimum details.
- If you receive an email that has information you know you should not have or that looks like a phishing attempt, notify your supervisor or IT staff. Phishing is another way hackers can get PII. Do not close the application or shut down your computer until it can be determined that it's not at risk.

Here's some startling data according to the Department of Education: In 60% of cases, attackers compromise an organization within minutes. Nearly 50% of people open emails and click on phishing links within the first hour. A campaign of only 10 emails yields a more than 90% chance that at least one person will click on the link. Malware attempts are largely focused on financial services, insurance, retail, utilities, and *education.*

(Guest article by WVNET staff member Dianne Sisler)

FROM THE DIRECTOR

With summer here already, WVNET is busy preparing for the West Virginia Statewide Technology Conference [details at wvstc.com]. We always enjoy the fellowship of seeing in person our customers and friends whom we mostly talk with by phone.

This has been a difficult month for all of us in West Virginia with our devastating floods that were so bad they made the national news. Our hearts and our prayers go out to all who were affected.

We hope you all are well or getting well and we hope to see you at the conference.

CUSTOMER SATISFACTION SURVEY

And this month's winner is...

I hope everyone had a safe and joyful 4th of July. I know that I personally enjoyed it with my wife and young son, maybe except for the fireworks late at night that kept him up when he doesn't sleep already. That wasn't fun. While we are enjoying ourselves, however, there are many public employees in the Mountain State that are continuing to keep critical processes and operations running. We take a minute and salute the forgotten many whose holidays constitute a heightened alertness for workdays usually marked by skeleton staffs. Without them, many of the things we take for granted on holidays would not be the case. Our survey winner this month was quite thankful that there were staff members on duty to assist him when he was working over the holiday weekend.

Each month, WVNET recognizes a customer who took the time to complete our Customer Satisfaction Service Survey to let us know how we are doing. We thank everyone who takes that extra few minutes to give us advice, kudos, or criticisms that will help us improve our service.

This month we would like to congratulate our winner, *Michael S. Lott, an employee for the Department of Natural Resources within the Law Enforcement Division*. While Mr. Lott called in with a password issue, and we were able to handle it and get him back on his system, he truly valued the fact that we were in the office and available during the holiday weekend. To quote Michael, *"Thanks for being there on a holiday; not all state employees work from* 9-5." We recognize that fact, Michael, and it is for you and other public employees who keep our State running strong that we have staff in place to assist 24/7/365.

There is not a day on the calendar that WVNET doesn't have the Network Operations Center staffed to assist customers with critical needs. In addition, the rest of our staff stands ready to support as second-level assistance should the need arise.

As always, at the end of each month, we will draw a winner, contact them by email and then send WVNET memorabilia in appreciation. Please complete our survey by looking within the incident email of any interaction that you have had with us. All comments are taken seriously and help to improve what we do on a daily basis.

Thank you, Michael, and thanks again to all our customers who continue to shape and improve WVNET.

(Guest article by WVNET staff member Booker Walton, III, pictured.)

'HUMMINGBAD' MALWARE HITS MILLIONS OF ANDROID DEVICES

A potent malware named HummingBad is spreading fast and is compromising user privacy by taking root in smartphones and tablets.

The HummingBad malware currently affects over 10 million Android smartphones and the only way to get rid of it is a factory reset.

Originating in China, HummingBad was created by a group of cyber criminals calling themselves Yingmob and has the potential to take root in your phone, install other fraudulent apps and generate fraudulent ad revenue by making it look like you clicked on certain mobile ads.

HummingBad can also steal information stored in your phone like texts, contacts, banking information and e-mail accounts, and its owners can sell such information to the highest bidder in the black market. According to security firm Check Point who published a research article on HummingBad, the malware has infected as many as 1.6 million devices in China, 1.3 million devices in India and around 100,000 devices including smartphones and tablets in the UK.

Check Point has also warned that Yingmob hackers can use HummingBad to carry out more direct and concentrated attacks in the future. "*Emboldened by this independence, Yingmob and groups like it can focus on honing their skill sets to take malware campaigns in entirely new directions, a trend Check Point researchers believe will escalate. For example, groups can pool device resources to create powerful botnets, they can create databases of devices to conduct highly-targeted attacks, or they can build new streams of revenue by selling access to devices under their control to the highest bidder,*" it said.

Given that HummingBad gains root access to your phone, it is not possible to simply uninstall it. Instead, you will have to make your phone or tablet undergo a factory reset after backing up your stored data. Installing a potent mobile antivirus software after rebooting your phone is recommended.

Keeping your version of Android up to date with the latest security patches helps to make it harder for the criminals to get a foothold on your device, as does not installing apps from anywhere other than the official Google Play store.

(Guest article by WVNET staff members Steven White, Randall Long and Barbara Long)

West Virginia Higher Education Technology Conference 2016 (WVHETC 2016) will be held September 26-27, 2016, at The Waterfront Hotel in Morgantown, WV. The conference theme is *"Transform Technology: Share, Educate & Secure."*

More details as they become available here: wvhetc.com

WVHETC
2016

NEW MAC MALWARE PROVES YOU SHOULDN'T DISABLE GATEKEEPER

Two discoveries in one week — a Mac malware boom

Security vendors are warning of two new types of malware for Apple computers that could have serious security impacts if inadvertently installed, but users who've kept Apple's default security configurations should be safe.

Enter Eleanor

The Backdoor.MAC.Eleanor malware, which was recently identified by Bitdefender researchers, sneaks onto your computer by posing as a harmless file converter called EasyDoc Converter.app.

Once on a Mac, Eleanor fires up a local web server. It also assigns each infected machine to a hidden Tor website. The attacker then can browse and control the infected computer through a web-based control panel. Hidden websites, signified by the ".onion" domain, offer more anonymity and are harder to trace to a specific hosting provider.

With Eleanor implanted, an attacker essentially has full control of the machine and can execute commands, turn on the webcam and send emails.

Eleanor does not have a digital certificate signed by Apple, which is good. That means if users have Apple's Gatekeeper set to only allow the installation of applications from the Mac App Store and identified developers - the default setting in OS X - it would be blocked.

Although security researchers have shown Gatekeeper can be fooled, it generally will block applications lacking a digital signature or ones that haven't been approved by Apple if it is configured to only allow downloads from the Mac App Store.

"In all, although this is a nasty bit of malware, the good news is that it's awfully easy to remove," writes Thomas Reed of Malwarebytes in a blog post. "*Further, the fact that it was disguised as a file converter meant to convert two relatively obscure file formats, coupled with the lack of any code signature, means that its distribution was probably fairly limited.*"

EasyDoc Converter was hosted on MacUpdate, a marketplace for Mac-compatible applications. EasyDoc Converter had user ratings that date back two years ago, Reed writes, but the malware only went live in April.

"I suspect that the real EasyDoc Converter may have been abandoned by its developer and somehow obtained by malware authors," he writes.

Keydnap Targets Keychain

Eleanor's appearance was quickly followed up by the third piece of Mac malware to appear so far this year. ESET, a security firm, calls it Keydnap, and it targets the Mac keychain, which is a very sensitive application.

That's because the keychain serves as a Mac's password manager, storing everything from router passwords to application and VPN passwords. It appears that Keydnap borrows proof-of-concept code published on GitHub, according to ESET malware researcher Marc-Etienne M. Léveillé. That code, written in October 2011 by Juuso Salonen, looks for master keys for the keychain in order to decrypt files.

Keydnap also seems to rely on social engineering. "*When two new processes are created within two seconds, Keydnap will spawn a window asking for the user's credentials, exactly like the one OS X users usually see when an application requires admin privileges,*" Léveillé writes. "*If the victim falls for this and enters their credentials, the backdoor will henceforth run as root, and the content of the victim's keychain will be exfiltrated.*"

The malware also uses Tor hidden services to communicate with its command-and-control server. ESET writes Keydnap may be distributed through spam messages or offered as a download on untrusted websites. The company is unsure how many people may have been infected. Keydnap does not have a digital certificate, so Gatekeeper will stop it. (Continued on next page...)

West Virginia NETWORK
Enhancing Education through Technology

Dan O'Hanlon, Director
837 Chestnut Ridge Road
Morgantown, WV 26505
304.522.7303
dohanlon@mail.wvnet.edu

Fran Barnes, Editorial Assistant
fran@mail.wvnet.edu

Also edited by:
Mike Karolchik, Manager
WVNET Media Services
mike@wvnet.edu

follow us on twitter

Follow @_wvnet

News

Newsletter Archives Here
www.wvnet.edu

(Continued from previous page…)

Apple Products Increasingly Targeted

While Mac users are targeted less by malware than Windows users, Mac aficionados should remain vigilant. For years, Apple portrayed its OS as being immune from the problems Windows users experienced. But as a 2015 study from Carbon Black showed, hackers are increasingly writing malware for Macs: *Five times more malware was found in 2015 than in the previous five years combined.*

Here are a few ways that you can protect yourself from being a victim of malware:

Do not disable Gatekeeper
Even though malware can sneak past Gatekeeper with a phony Developer ID, enabling it will not hurt. It would also be best to limit downloading applications from third parties all-together. If you can find what you need on the official AppStore, it would be safer to get it from there.

Browser Security
Be careful about the websites you visit, what links you click on, and what you download. Also, watch out for suspicious looking emails and attachments.

Patch and Upgrade
It is essential to update your OS and software because each update includes patches that help protect against the malware attacks that Apple knows about.

(Guest article by WVNET staff members Steven White, Randall Long and Barbara Long)

"So Long, Farewell…"

Seventeen-year cicadas spend over 99 percent of their lives underground, only to crawl out by the billions on a warm spring night in their 17th year. Then, after dedicating a few weeks to repopulating the brood, their bodies fall back to the ground they emerged from. Here are 17 facts about the periodical bugs worth knowing…

- **They're active their whole lives.**
- **Their diet may explain their long lifestyle.**
- **They use trees to keep track of time.**
- **Math helps them avoid predators.**
- **They evolved during the last ice age.**
- **They're triggered by temperature.**
- **There are 12 different broods.**
- **They arrive in large numbers.**
- **They're a treat for humans, too.**
- **They leave a lot of exoskeletons behind.**
- **They're not locusts.**
- **Their songs can reach 100 decibels.**
- **They're attracted to power tools.**
- **They lay their eggs in tree branches.**
- **They're one of the oldest insects.**
- **They have five eyes.**
- **Every 221 years, 13-year and 17-year cicadas co-emerge.**

…See you in another 17 years.