Play Your Way to Success: Building Tomorrow's Workforce

NICE Working Group Competitions Subgroup

Laurin Buchanan
Secure Decisions

Jake Mihevc
Mohawk Valley Community College

Dan Manson
Cal Poly Pomona

Amelia Phillips
Highline College
NIST NICE Working Group (NICEWG)

Provides mechanism in which public and private sector participants can
• develop concepts
• design strategies
• pursue actions that advance cybersecurity education, training, & workforce development

3 Co-Chairs: Academia, Industry, Government

5 Sub-Working Groups
NICEWG Competitions Sub-Group Mission/Vision

**Vision:**
Promote a spectrum of competitions that advances knowledge, skills and abilities to nurture and expand a diverse national talent pool.

**Mission:**
Empower a public and private competition ecosystem by providing guidelines, standards, and best practices for players, teams, schools, sponsors and organizers.
Competitions and games come in all flavors.
Case Study: Attracting interest in cyber careers
What: introducing kids to cyber issues and roles

Who: Middle school kids
Where: Community center
When: After school
How: Branching web comics show how cybersecurity affects everyone
Why: Get kids interested in cyber

Comic-BEE 🐝
We only found one piece of malware at FirstBank, on a manager's computer.

But every malware has a unique "signature" - like fingerprints - that tells us about it. We can use that to find other incidents with this malware.

**NBI Malware Analysis System**

**Signature Report**

*Submitted by:* Melissa Adrien  
*Case:* FirstBank  
*Filename:* %Temp%\iexplore.exe

**MALWARE TYPE**

- General Trojan: .08% = No
- Banking Trojan: .05% = No
- Virus: 0% = No
- Worm: 0% = No
- Ransomware: .02% = No
- Rootkit: 0% = No
- Common: 40% = Yes
  
(spam, spyware, adware)

**Hmmm,**  
this malware doesn't do anything special.  
This doesn't tell us much!
We only found one piece of malware at FirstBank, on a manager's computer.

But every malware has a unique "signature" - like fingerprints - that tells us about it. We can use that to find other incidents with this malware.

Ding! Analysis complete

How do you learn more about the malware?

Try to run the malware in the lab

Look for similar malware in other investigations

NBI Malware Analysis System
Signature Report

Submitted by: Melissa Adrien
Case: FirstBank
Filename: %Temp%\explore.exe

MALWARE TYPE

General Trojan: .08% = No
Banking Trojan: .05% = No
Virus: 0% = No
Worm: 0% = No
Ransomware: .02% = No
Rootkit: 0% = No
Common: 40% = Yes
(spam, spyware, adware)

Hmmmm, this malware doesn't do anything special. This doesn't tell us much!
I've isolated the malware. Let's see what it does in the lab network... I'll put it on virtual machine first.

OK - sometimes malware doesn't trigger in a virtual machine. I'll try a physical machine.

This malware just isn't doing anything. What am I missing?

Virtual Machine (VM) Analysis System Report
- 08:00 - Scan: no malware detected
- 08:10 - VM reboot
- 08:23 - Scan: no malware detected
- 08:30 - VM reboot
- 08:35 - Scan: no malware detected

Forensic Framework System Analysis Report
- 10:01 - Scan: no malware detected
- 10:10 - VM reboot
- 10:28 - Scan: no malware detected
- 10:35 - VM reboot
- 10:49 - Scan: no malware detected
I've isolated the malware. Let's see what it does in the lab network... I'll put it on virtual machine first.

OK - sometimes malware doesn't trigger in a virtual machine. I'll try a physical machine.

This malware just isn't doing anything. What am I missing?

Virtual Machine (VM) Analysis System Report

08:00 - Scan: no malware detected
08:10 - VM reboot
08:23 - Scan: no malware detected
08:30 - VM reboot
08:35 - Scan: no malware detected

Forensic Framework System Analysis Report

10:01 - Scan: no malware detected
10:10 - VM reboot
10:28 - Scan: no malware detected
10:35 - VM reboot
10:49 - Scan: no malware detected

So that didn't work - what do you want to try next?

- Analyze systems of FirstBank's customers
- Look for this malware in other investigations
Hey, Melissa - looks like we found your malware in another investigation! Look at the image on this USB.

Time to explore this new computer image in our Forensics Framework - let's see what's here.

Here's the main executable file that gives the malware its instructions. Let's see what processes and files it interacts with.

This file interacts with another file! This malware may be modular - with parts that can be separated and recombined. We need to be looking for this DLL.

Dynamic Trace Analysis of file: %Temp%\iexplore.exe

Interactions
rberman.dll
Hey, Melissa - looks like we found your malware in another investigation! Look at the image on this USB.

Time to explore this new computer image in our Forensics Framework - let's see what's here.

Here's the main executable file that gives the malware its instructions. Let's see what processes and files it interacts with.

This file interacts with another file! This malware may be modular - with parts that can be separated and recombined. We need to be looking for this DLL.

Dynamic Trace Analysis of file: %Temp\ieexplore.exe

Interactions
rberman.dll

How do you expand your investigation to include this new .dll file?

- Ask malware specialist to analyze the .dll file
- Look for the .dll file in the images you have from the bank and its customers
- Look for that .dll file in any other recent investigation
Web comics are popular with everyone

Positive “first contact” experience is critical to continued interest in next stage

• Learn while having fun
• Literally “see yourself” in comics – critical for developing self-efficacy

Go beyond reading comics: much deeper engagement when learners create their own comics
Failure always an option - and bigger is better with comics!

Memorable or exaggerated endings reinforce learning

Story format shows consequences of choices immediately: not bound by reality of time and distance

Experience consequences of bad decision in a safe environment
Case Study: Competitions as part of formal education
Mohawk Valley Community College (MVCC)

MVCC: CAE 2Y
Utica College: CAE-CDE
SUNY Polytechnic
Air Force Research Lab in Rome, NY

Central New York (CNY) Hackathon: 1 event each semester
CNY Hackathon

8 different colleges participate

Teams composed of students from each college

Competition elements
• Infrastructure (CCDC)
• Capture The Flag (CTF)
• Wireless Challenge
Competitors develop more than technical skills

Soft skills:
• Leadership
  Team Leaders – HANDS OFF
• Teamwork
  Teams created by script

Students learn WHY they need to learn networking, operating systems and coding so well
Students are engaged

Students learn where they stand - need to work harder?

Students WANT to come back better next year
Benefit to MVCC goes beyond enrollment

Industry develops CNY exercises
• Provides DIRECT alignment with workforce needs
• Faculty update curriculum 2x year!

Students see path:

Strong performer  Employment  Red Team

Cybersecurity Enrollment

Strong performer  Employment  Red Team

Cybersecurity Enrollment

1  2  3  4  5  6
0  20  40  60  80  100  120  140  160  180
Benefit to student’s next stage of development

Cyber is such an APPLIED discipline — it is uniquely geared toward competency-based education.

Competitions map to Security+ and Certified Ethical Hacker “scenarios” later in careers.
Failure at CNY Hackathon?

Failure to work as a team
Failure to learn anything
Failure to be ethical

Success at CNY Hackathon:
Great team comes together OR epic failure leads to lessons learned!
Case Study #3: Practice, training and education for the cyber workforce
National Cyber League

Provides an ongoing virtual training ground for participants to develop, practice, and validate their cybersecurity knowledge and skills

NCL uses next-generation, high-fidelity simulation environments

Blog at cryptokait.wordpress.com
Kaitlyn Bestenheider encourages women and girls in this male-dominated field and shares her experiences:

"I hope to help students gain the confidence to sign up for their first Capture-the-Flag (CTF) competition. I think NCL is the best CTF for students to do because it’s designed to be accessible for first-time cybersecurity students and still be challenging to prepare them for the workforce."
Nevada Cyber Club (NCC)

NCC-1701 team competed in NCL

At 3-day national competition, NCC-1701 came in 2nd place out of 264 teams, missing only one of 161 problems

“I enjoy having an environment where I need to be a part of a team with different skill sets to solve challenging and hands-on problems.”
— Alexander Parr, VP NCC team, NCL player
Paradigm shift needed to address “The Gap”

Growing gap: demand vs. supply of well-qualified cyber professionals

Technical/ virtual environments are important
• Key training for doctors, pilots, emergency professionals, professional athletes

Brain science shows repetition is essential to knowledge retention
• Muscle Memory: repeating tasks over and over enhances neural pathways
• Multiple avenues mean more neural pathways & stronger retention
‘Gamification’

Introduces concepts of games into real-world education, training and assessment environments

• Encourages repetition
• Provides positive incentives, not just negative ones  
  >> makes training “sticky”
• As skills improve, challenges should too!
What a good cyber competition can do

- Raise public awareness about cyber competitions
- Exponentially multiply number of cyber games, sponsors and participants
- Inform and restructure academic curricula
- Transform and popularize specific cyber training strategies
- Aid recruiters in identifying talent
Raise awareness: broadcasting cyber competitions

Recent global competition in Las Vegas: 2 hour LIVE filmed competition

Congratulations to all winners — including Las Vegas’ own Monique Moreno, College of Southern Nevada
Case Study: Advanced, professional cyber competitions
Emerald Down regional exercise

Began at urging from David Matthews – Deputy CISO, City of Seattle

Pacific North West Economic Region: cyber as an interdependency

First conducted in 2012

- 8 teams live at King County Emergency Operations Center in Renton; other teams in their own locations
- Scenario: Major IT issue, compromised firmware
- IT teams from various organizations
Academia, Government and Industry participated

Various organizations had to cooperate with one another
• Many not used to reaching out
• Learned what other organizations could do

Developed new partnerships and contacts
• Cyber Incident Response Coalition and Analysis Sharing (CIRCAS): public-private cyber resilience coalition
Emerald Down V: table top exercise

Board game simulated real-life network compromise
Elements of Emerald Down V

- Elements of luck, timing, relative power, etc.
- Game both fun and very enlightening to participants
- Facilitators kept game moving
- Students as Evaluators

Very unique: different levels of government and military had access to varying levels of response

Fascinating to watch: https://vimeo.com/207705607
Extended benefits of advanced exercise

Practiced community cyber security response approach with interactive exercise

Developed Cyber Annex to WA State’s Comprehensive Emergency Response Plan — first in the nation, noted by FEMA & other jurisdictions

Organizations explore how their Cyber Plans could integrate with WA State’s Cyber Annex to Emergency Response Plan

Build trust among technology and security practitioners
Failure is the way to success!

Outcome of exercise is to update the Emergency Management Response plan

Failure identifies where the gaps are

Fix them!
Questions?
Competitions Subgroup deliverables

https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/competitions-sub-working-group

One-Pager on Competitions

Cybersecurity Games White Paper

Letter: “Ten Things Parents Need to Know about Competitions”

Links to competition podcasts

Survey on cyber competitions:
https://www.surveymonkey.com/r/YPXPX8V