Making and Breaking NSA's Codebreaker Challenge

Rita Doerr, Ph.D.
Academic Outreach Lead
NSA's Cybersecurity Directorate

A Pictorial Bio

Can You Find the Pattern?

5   14   329   481   539   377   531   452   631   449

Takeaways …

- **Impact #1**: ? ? 5 5 2 13 136 61 185 101 …

- **Impact #2**: CBC influences post-secondary education!!

- **Impact #3**: 1000+ applicants; hundreds offered jobs!!

Historical Motivation

- 10+ years ago …
- NSA Academic Liaisons
- Visit colleges / universities around the US
- Recurrent theme … “what does NSA do??”
- Need some ***UNCLASSIFIED*** problem
    - ➢ Codebreaker Challenge (CBC) was born

What? Codebreaker Challenge

- Annual cryptanalytic & cyber competition
- NSA academic outreach & recruiting effort
- “… to give **university students** exposure to unclassified problems that simulate the classified work performed at NSA.”

Why? Codebreaker Challenge

- It provides a realistic, NSA mission-centric scenario that inspires students to develop or master their technical abilities
- An experiential learning innovation aimed at bolstering available resources for cybersecurity education
- A ‘recruiting & hiring’ tool to help identify top talent
  - ➢ Teaser – see Impact #3

Who? Codebreaker Challenge

- **Participants**: open to schools based in US or territories (register with your school email address)

- **Designers / Developers / Deployers**: NSA employees
  - ➢ 2-3 days of initial brainstorming with 10-12 ‘volunteers’
  - ➢ 3-4 weeks to design overall ***<u>FICTITIOUS</u>*** scenario & mission
  - ➢ 4-5 months to develop/implement & deploy entire challenge

When? Codebreaker Challenge

- Runs throughout the fall semester
    - **August – December**

- Design / Develop / Deploy
    - **January – July**

How? Codebreaker Challenge

- **Structured**:
  - ➢ A series of successively harder ‘tiers / tasks’ that closely mirror the real-world scenarios that NSA analysts deal with every day
  - ➢ One tasks gives ‘hints / insights’ into the next ☺
- **Scored**:
  - ➢ Student Participants: earn points for each completed task
  - ➢ Schools: accumulate points from all student participants (from the same school)

CBC by the Numbers

Year	Total Participants	Total Schools/Districts	Total Solvers
2013		5	
2014		14	
2015	2217	329	54
2016	3325	481	15
2017	3103	539	3
2018	2850	377	18
2019	3777	531	50
2020	3156	452	6
2021	5465	631	38
2022	4803	449	104

CBC Scenarios

2013

- Reverse-engineer a program which prompted for a password
- Needed AES key derived from SHA256 hash
- **NOTE**: each participant received a unique binary

CBC Scenarios (cont.)

2014 / 2015

- International terrorist orgs revised OPSEC procedures to their operatives in the field using a program being used to covertly encrypt messages

CBC Scenarios (cont.)

2016

- Terrorists have developed a new IED (Improvised Explosive Device) making it harder for US military to detect and prevent roadside attacks

CBC Scenarios (cont.)

2017

- DHS (Department of Homeland Security) has requested NSA’s assistance in investigating a potential intrusion into critical US infrastructure

CBC Scenarios (cont.)

2018

- A new strain of ransomware has managed to penetrate several critical government networks and NSA has been called upon to assist in remediating the infection to prevent massive data loss

CBC Scenarios (cont.)

2019

- Reverse engineer and develop new exploitation capabilities against *TerrorTime*, a custom Android secure messaging app

CBC Scenarios (cont.)

2020

- Two days ago, a renowned American went missing on an assignment abroad
- Local street surveillance cameras recorded footage of incident as well as cell phone of journalist being destroyed

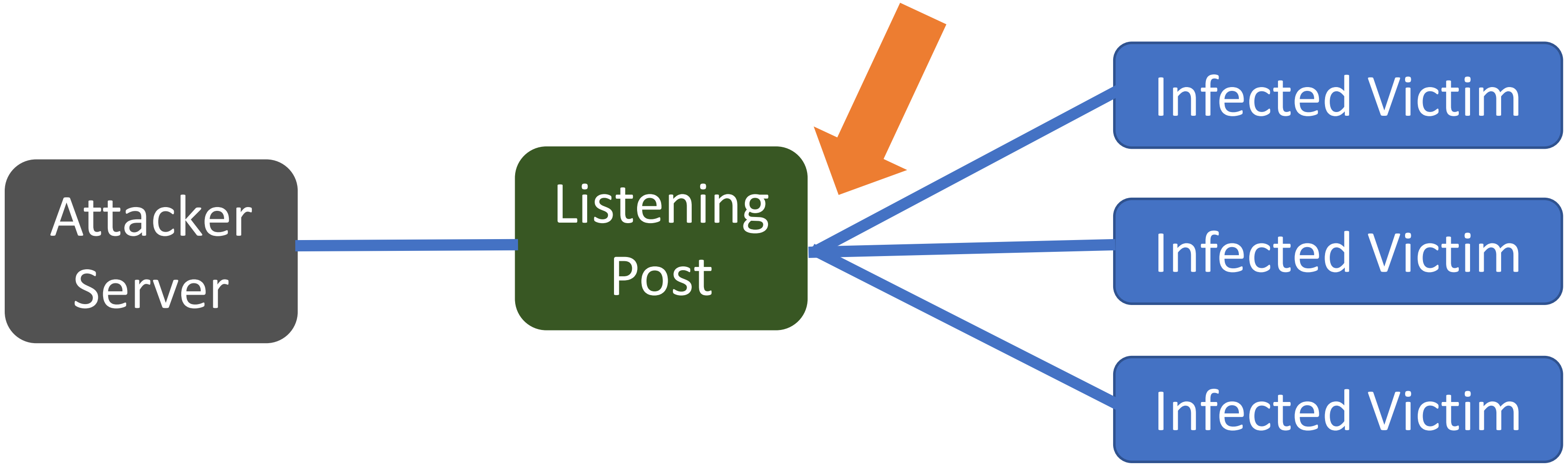
CBC Scenarios (cont.)

2021

- NSA was investigating a foreign cyber actor
- Identified suspicious IP address and captured network traffic going towards it
- NSA believes that the machine is one of the actor’s ‘listening posts’

Aside: Listening Post

- Synonym for command and control (C2) server
- Attacker-controlled server, communicates with attacker's malware



Top CBC Solvers

	Schools	# of Solvers
2013		
2014		
2015	Georgia Institute of Technology	7
2016	Georgia Institute of Technology	5
2017	Carnegie Mellon University	2
2018	Georgia Institute of Technology	3
2019	University of North Georgia	30
2020	6-way tie	1
2021	Georgia Institute of Technology	8
2022	Georgia Institute of Technology	19

2022 Scenario

- A company’s internal network has been taken over by ransomware

- They call the FBI, who asked NSA for technical assistance

2022 Mission

- **Find** the attacker’s identity
- **Identify** the tools that they used to carry out their attack
- **Investigate** a Ransomware-as-a-Service (RaaS) website used by the attacker
    - ➢ **Find** and **Exploit** vulnerabilities to recover the victim’s files

2022 Tasks

Tasks A1 – A2: Investigate the Victim’s Network

- Task A1: Which user account was **compromised**? (Log Analysis)

- Task A2: **Recover** the attacker’s tools and discover their identity (Network and File Forensics)

2022 Tasks (cont.)

Tasks B1 – B2: Investigate the Ransomware Site

- Task B1: **Locate** RaaS website (Web reverse engineering)

- Task B2: **Find** more information about the RaaS site (Web analysis & exploitation)

2022 Tasks (cont.)

Tasks 5 – 6: Gain access to the RaaS Site

- Task 5: **Recover** information from the attacker’s computer (Reverse Engineering, Cryptanalysis)

- Task 6: **Access** the RaaS site as the attacker (Web Hacking)

2022 Tasks (cont.)

Tasks 7 – 9: Recover the victim's keys

- Task 7: **Escalate** privileges to an administrator account (Web Hacking)

- Task 8: **Find** the key-encrypting-key used to protect the keys that encrypt victim's files (Web Hacking, Reverse Engineering)

- Task 9: **Recover** the victim's keys (Cryptanalysis, Software Development)

2022 Skills Learned

- Forensics (network, host)
- Binary Reverse Engineering
- Web Analysis and Exploitation
- Cryptanalysis
- Software Development

CBC Impact #1

	Total Participants	High School Participants*
2013		
2014		
2015	2217	5
2016	3325	5
2017	3103	2
2018	2850	13
2019	3777	136
2020	3156	61
2021	5465	185
2022	4803	101

* Counted by searching for ‘School’, then manually filtering; generally can’t distinguish between high school and below

CBC Impact #2

Several post-secondary schools:

- Used [some of] the CBC technical resources as part of their cybersecurity curriculum

Other post-secondary schools:

- The CBC enabled students to obtain credit for a course’s final exam if they successfully solved the entirety of the Challenge
- The CBC steers which topics are covered within cyber and computer science courses

CBC Impact #3 – the 'So What'?!

Since CBC inception in 2013:

- 965 Applicants
- 432 Conditional Job Offers
- 140 Final Job Offers

DISCLAIMER: numbers are *lower bounds*, where CBC email address = email address on NSA application

Coming Soon: CBC 2023!!

- **Scenario**: US Coast Guard discovered an unknown signal 30 miles OCONUS. NSA is asked to interpret and discover the origin of the signal.
- **Number of Tasks**: 9
- **Timeframe**: September 28 - December 21, 2023
- **Visit**: `nsa-codebreaker.org`
- **Check Out**: NSA Twitter, Facebook, LinkedIn, Instagram

Black Hat Sound Bytes

- **Participants**: high school students!!
- **Cyber/CS Curriculum**: CBC driving content!!
- **Hiring**: thousands have applied; hundreds offered jobs!!

Acknowledgements

- Aaron H
- Ben M
- Eric B
- Josiah D
- Michelle I

✓ Pamela O’Shea (Black Hat Speakers Coach)

Questions?

Thanks for your time!