Ok HEADQUARTERS PHILIPPINE NAVY
OFFICE OF THE AC OF NS FOR C4ISR SYSTEMS, N6
Naval Station Jose Andrada
2335 Roxas Boulevard, Manila

From: Staff Officer, Cyber Warfare Management Branch
To: AC of NS for C4ISR Systems, N6
Via: Deputy AC of NS for C4ISR Systems, N6

Subj: Attendance to RootCon Hackers' Conference

Ref: FOIC, PN approved DF dated 02 August 2019, subject: Attendance to RootCon Event

Encls:
1) Topic Presentations
2) AAR from LTJG MARIO N TRIBUNAL PN
3) Pictures with caption

I. General:

ROOTCON is an annual cyber security conference and the largest hacking conference in the Philippines. The event aims to foster camaraderie and sharing of expertise among cybersecurity professionals, security researchers, and ethical hackers. A two-day activity showcasing lectures on the latest techniques and tactics of hacking, a hands-on experience on ways of cracking devices; and competing in the Capture the Flag (CTF) contest - a special kind of cybersecurity competition designed to challenge its participants to solve computer security problems.

This activity was held on 26-27 September 2019 at Taal Vista Hotel, Tagaytay and was attended by LCDR RODEL G BARRACA PN, CPT JEAN PAUL T SAN GABRIEL PN(M), LTJG MARIO N TRIBUNAL PN, LTJG JOMAR M WELBA PN, SN2 Rhea T Espinosa PN, and Mr. Nelson G. Maligro CE.

II. Schedule of Activities:

Time	Activities/ Topics	Resource Person
Day 1		
0900H-0930H	Keynote	CDR LOPEZ, Commander, AFPCYG
0930H-1015H	Navigating the Shift from Opportunistic to Targeted Ransomware	Christopher Elisan
1015H-1115H	Capture The Flag (CTF) game participated by ON6 and NICTC personnel.	
1115H-1215H	Farewell, WAF - Exploiting SQL	Boik Su

	Injection from Mutation to Polymorphism	
Lunch		
1300H-1345H	The Man-In-The-Middle attack against a certain password manager	Soya Aoyama
1345H-1430H	Pilot Study on Semi-Automated Patch Diffing by Applying Machine-Learning Techniques	Asuka Nakajima
1430H-1545H	SAML Assailant	Narayan Gowraj
1545H-1645H	Identity crisis: war stories from authentication failures	Vishal Chauhan
Day 2		
0900H-0930H	Speed Talk about the upcoming ISOG event which includes Defense the Flag (DTF) game	Information Security Officers Group (ISOG)
0930H-1015H	Dissecting APT Malware against Taiwan in 2019	Bletchley Chen & Inndy Lin
1015H-1100H	Behind LockerGoga – A walk through a ransomware attack	Magda Lilia Chelly
1100H-1200H	Hunting Threats with Wireshark Plugins	Nishant Sharma, Jeswin Mathai, & Shivam Bathla
Lunch		
1300H-1345H	Hacking ICS devices/PLC's for Fun - ICS and IOT Hacking	Arun Mane
1345H-1430H	z3r0 to h3r0 - Targeting Crown Jewels over the Internet	Viral Maniar
1430H-1530H	Making Anomaly Detection system(ADS) for Vehicles (Automotive Hacking)	Arun Mane & Nikhil Bogam
1530H-1630H	Awarding and Closing Remark	Dax Labrador aka Semprix, Founder RootCon

III. Fund Support:

Training fees and hotel accommodation were provided by this office.

IV. Observations/Lessons Learned:

The RootCon event was an eye-opening experience to ON6 and NICTC personnel. The presenters unselfishly shared their experience on the latest techniques on breaking a system, carving advanced malware such as the APT, and effective ways of hunting threats.

The following are the topics that were discussed:

1. Navigating the Shift from Opportunistic to Targeted Ransomware

- Attackers have been hitting organizations hard by flooding ransomware onto computers and network shares; and demanding drastically high ransoms in return for decrypted data.

2. SQL Injection from Mutation to Polymorphism
   - A brief introduction of the mutation technique, the differences among other evasion techniques, the scheme, the algorithm, and the potential risks it may raise in the future.

3. Semi-Automated Patch Diffing by Applying Machine-Learning Techniques
   - Patch diffing (binary diffing) is one of the major techniques to identify that security fixes are applied. Various tools include BinDiff, TurboDiff, and Diaphora have been developed.

4. Hunting Threats with Wireshark Plugins
   - Converting our traffic analysis tool Wireshark, to an extensible, free platform independent threat/signature/attack hunter tool

5. Man-In-The-Middle attack against a certain password manager
   - Man-in-the-middle attack against a certain password management application. The password was exchanged in plain text between .exe and .dll, and it was very easy to steal it.

Aside from lectures, various activities were also conducted during the two (2) days event. Below are note-worthy observations:

1. Villages or booth were setup to provide hands-on experience on fixing and soldering Arduino boards, lock picking, and car-jacking. This is to provide awareness to the participants on how real the threats are.

2. There is a separate room for learning basics of hacking.

3. Advance methodologies were presented straight from recognized ethical hackers and security researchers. These lecturers had previously spoken at DEFCON, SECCON, and BlackHat– a US hackers' conference.

4. Separate track for the Capture the Flag (CTF) game participated by skillful hackers in the Philippines. The team from PN had the opportunity to join the CTF under the name "Hard&Soft" – Hardware and Software. The PN team experienced the grueling annual Rootcon's hackers' competition and learned the need to advance into reverse engineering, web exploitation, forensic and cryptography.

5. The Hackers' Night sponsored by Microsoft provided a venue to fraternize with fellow cyber security professionals, security researchers, and other discreet hackers.

V. Recommendation

In view hereof, this branch recommends the following:

<u>NICTC:</u>

1. NICTC should put more emphasis on lab-intensive and core competency trainings to enhance the skills and have a vivid understanding of the emerging threats.

2. NICTC shall program in their APB the attendance to RootCon.or similar hackers' conferences. It will allow them to learn new techniques and will have the opportunity to engage with some of the hackers in the Philippines.

3. NICTC should develop cybersecurity competencies with dedicated area of expertise such as reverse engineering for malware analysis, web exploitation for testing PN web app security, computer forensic, cryptography, etc.

ON6:

4. Subscribe to the PenTesters Academy – an online penetration testing laboratory - to train technical personnel on ways of finding vulnerability and gaining access into the system. This will also prepare the Hard&Soft team for the next CTF.

5. Continues attendance to RootCon.

1589183344211

RODEL G BARRACA
LCDR PN