Monthly Research

CODE BLUE 2015 Report

FFRI, Inc.

http://www.ffri.jp

Ver 1.00.01

Introduction

- The international security professional conference CODE BLUE 2015 was held in Tokyo October 28-29.
- More than 600 people were attended this 3rd CODE BLUE.
- Our researchers also announced research results in this CODE BLUE.
- We show about CODE BLUE 2015 and interesting presentations.

Agenda

- CODE BLUE 2015
- Presentations of FFRI researcher
- Security threats in IoT
- Bug Bounty state-of-the-art
- Rapidly increasing Advanced Persistent Threat (APT)
- New challenge Youth Track
- Summary

CODE BLUE 2015

- Two new challenges
  - 2 track
    - Parallel 2 presentations of different themes
  - Youth Track
    - Presentation by less than 25-year-old researcher

Presentations by FFRI researcher

- **iOS malware trends and the malware detection with the dedicated gadgets**
  - **Motoki Nishio**

- **Threat Analysis of Windows 10 IoT Core and Recommended Security Measures**
  - **Naohide Waguri**

- Further details will be announced later on http://www.ffri.jp/research

Security threats in IoT

- **(In)Security of Medical Devices**
  - Florian Grunow is a security analyst at ERNW.
  - He presented cyber attacks targeted medical equipment.
  - He attacked equipment to adjust the dosage and measurement instruments used during surgery.

- **Wireless security testing with attack**
  - Keiichi Horiai presented the attack on the wireless technology using the SDR(Software Defined Radio).
  - He showed about GNURadio and the replay attack for RF signal, sniffer for wireless keyboards with some demos.

Security threats in IoT (cont'd)

- **Cybersecurity of SmartGrid**
  - Aleksandr Timorin is security researcher, author of ICS/SCADA network security toolkits.
  - Sergey Gordeychik is the Director and Scriptwriter of the Positive Hack Days forum, captain of SCADAStrangeLove.org team and Web Application Security Consortium (WASC) contributor presented about smart grid security.
  - They showed safety assessment of the various elements of smart grid technology from solar power generation system to digital substation.

Bug Bounty state-of-the-art

- **Defeating Firefox**
  - Muneaki Nishimura, also known as Nishimunea, is a security researcher and weekend bug hunter.
    He got about 60,000 USD bounties in this year.
  - He presented pattern of vulnerability and finding method.
  - Many browsers do not meet the requirements defined in the RFC at first.
  - Therefore, many vulnerabilities are found at new functions.
  - When new functions had been released you can found vulnerabilities with specifications based testing.

Bug Bounty state-of-the-art (cont'd)

- **X-XSS-Nightmare: 1; mode=attack XSS Attacks By Abusing the XSS Filter**
  - Masato Kinugawa has the number of reports of the world second place in Google‘s bug bounty program and reported vulnerabilities to many products.
  - He presented about new XSS technique using “XSS Filter” in Internet Explorer and Edge.
  - XSS Filter is rewriting part of pages to prevent XSS.

    He exploited this for html tag breaking XSS.
  - There was no referral for specific attack methods in the his presentation.
  - But if finishing coordination with Microsoft, it will be published.

Rapidly increasing APT

- **Revealing the Attack Operations Targeting Japan**
  - Shusei Tomonaga and Yuu Nakamura are analyst of JPCERT/CC
  - They are presented about APT operations targeting Japan.
    - Emdivi and the another advanced case
  - Latest attack techniques and malware and attack tools
    - The attacks utilizing the iptables not to leave any traces
  - They also showed analyzing techniques and tools for APT.
    - IDA Python script for analyzing Emdivi
    - It's published on GitHub now.

Rapidly increasing APT (cont'd)

- **Ninja Correlation of APT Binaries**
  - Bhavna Soman presented a variety of techniques suitable for evaluating actual code similarity malware specimens used in the APT.
  - Create a cluster of binary that each specimen of similarity metric based on, such as technology to evaluate its accuracy has been introduced.
- **Failures of security industry in the last decade - Lessons learned from hundreds of cyber espionage breaches**
  - Sung-ting and Chi-en Shen presented about cyber attacks with a focus on Asia.
  - They showed concrete cases of cyber attacks as about Japan Pension Service, and how attackers break the security measures.

New challenge Youth Track

- **PANDEMONIUM: Automated Identification of Cryptographic Algorithms using Dynamic Binary Instrumentation and Fuzzy Hashing**
  - Yuma Kurogome presented about automatic identification of malware encryption algorithm using fuzzy hashing.
  - Zeus’s source code was leaked and various variants have produced.
  - He introduced a method of extracting portion that contains encryption process by focusing on such as arithmetic bit operations and loop structure in which these malware do.
  - He also showed the avoidance technique of analysis interference function using LLVM.
  - His technique disables anti-analysis function using the fuzzy hashing.

New challenge Youth Track (cont'd)

- **Master Canary Forging: A new exploitation method to bypass stack canaries**
  - Yuki Koike who is a student at Nada High School in Japan, many CTF finalist and champion presented about new bypass technique of stack canary.
  - Previously, the main methods to bypass stack canaries were to exploit different vulnerabilities to either avoid the canary validation completely, or to provide the correct canary value by leaking the value.
  - He proposed a new technique to bypass stack canaries in SSP which takes a different approach from the previous methods.
  - He showed rewriting of master canary with demo.

Summary

- CODE BLUE 2015 had over 600 visitors from many countries.
  - It had started two track presentation and youth track.
  - Two teenagers and a student were on stage.
- IoT Security
  - Medical equipment and social infrastructure were studied.
  - The white hackers reported these vulnerabilities.
- Bug Bounty
  - Japanese bug hunters are active in the world.
  - There are things to learn from their way.
- APT
  - APT would have invaded various organizations in Japan.
  - Forum for information exchange, such as the CODE BLUE is required to counter APT.

References

- SPEAKERS || CONTENTS || CODE BLUE : International Security Conference in Tokyo where Global Security Trends, Top Notch Professionals, and participants intersect http://codeblue.jp/2015/en/contents/speakers.html

Contact Information

E-Mail : research—feedback@ffri.jp
Twitter : @FFRI_Research