AFRL-OSR-VA-TR-2013-0159

Internet attack traceback: cross-validation and pebble-trace

David Lee and Ten H. Lai
Ohio State University

April 2013
Final Report

AIR FORCE RESEARCH LABORATORY
AF OFFICE OF SCIENTIFIC RESEARCH (AFOSR)
ARLINGTON, VIRGINIA 22203
AIR FORCE MATERIEL COMMAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
28/02/2013	FINAL REPORT	01/04/2009 - 30/11/2012

4. TITLE AND SUBTITLE

Internet attack traceback: cross-validation and pebble-trace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

FA9550-09-1-0280

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

David Lee and Ten H. Lai

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The Ohio State University
Department of Computer Science and Engineering,
2015 Neil Ave., Columbus, OH 43210

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

AFRL-OSR-VA-TR-2013-0159

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A: APPROVED FOR PUBLIC RELEASE

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On the Internet, attackers often launch attacks through stepping-stones to steal confidential information from victims. Hiding behind stepping-stones, attackers thus avoid being traced back. In this project, the problem of Internet attack traceback was studied. A Pebbletrace scheme was proposed, which imbeds zero-day based Pebbleware in the stolen information and thereby enables one to trace back to the attacker's machine which has the stolen information.

A Pebbletrace prototype was built and focused on two cases: (1) the attacker steals a PDF file and (2) the attacker steals sensitive information through Zeus botnets. In the two cases, the project showed how to create Pebbleware automatically based on zero-day vulnerabilities, and how Pebbletrace reveals attackers whose machines are vulnerable to these zero-days.

15. SUBJECT TERMS

Traceback, zero-day vulnerability, Pebbleware, Pebbletrace, botnet.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Ten H. Lai
U	U	U	SAR		19b. TELEPHONE NUMBER *(Include area code)* 614-292-2146

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

THE OHIO STATE UNIVERSITY

Internet attack traceback: cross-validation and pebble-trace

AFOSR Project Final Report

David Lee and Ten H. Lai

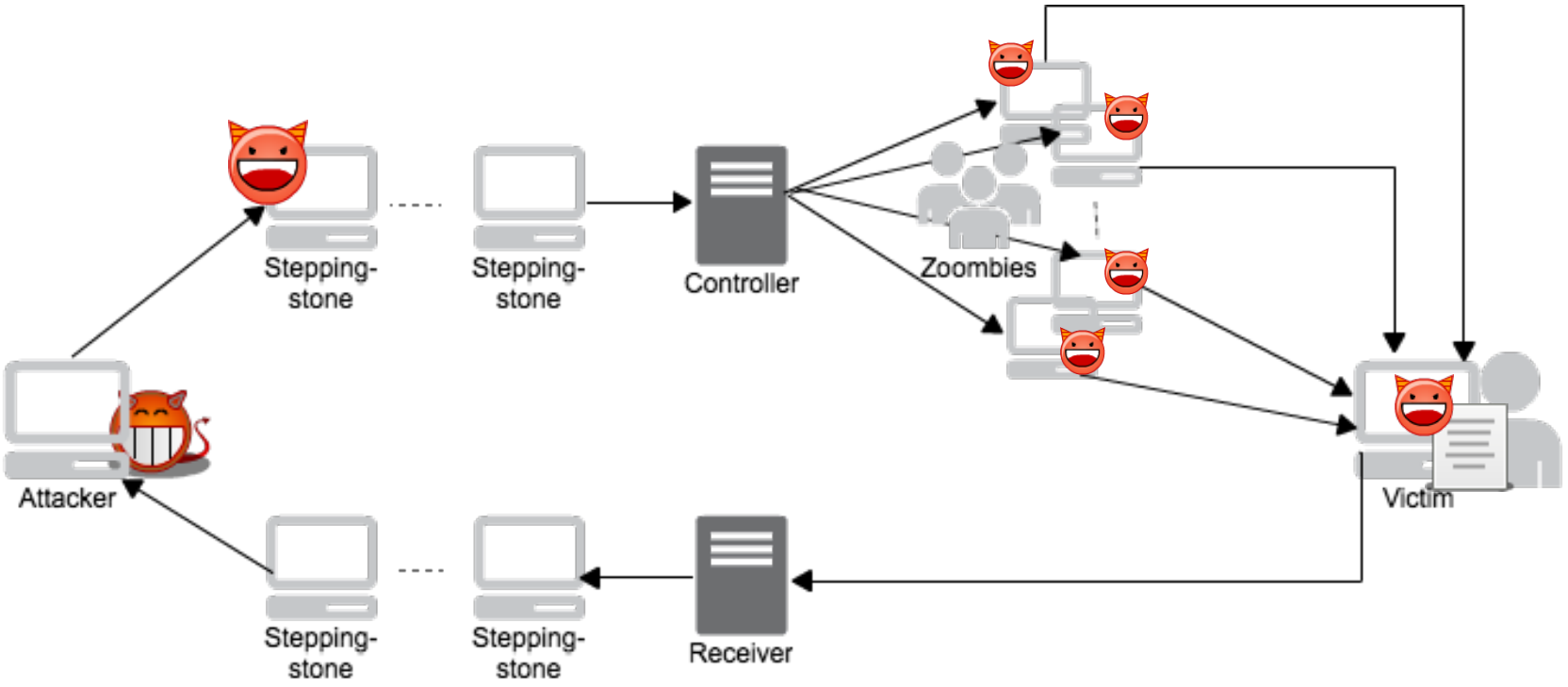
The Ohio State University

February 28, 2013

Outline

- Traceback Internet attacks
  - Problem
  - Challenges
- Our solution: Pebbletrace
  - Steal files
  - Steal information
- Conclusion

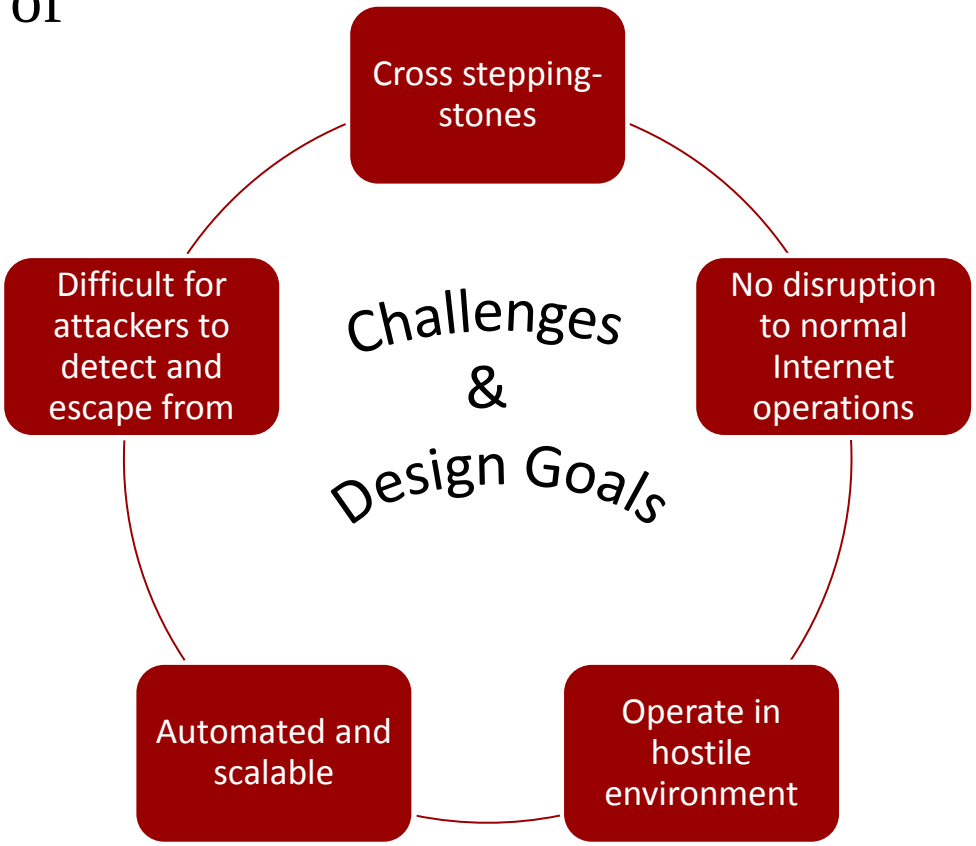
Model of Internet Attacks



Attacker attempts to steal confidential files/information

Attack Traceback

Trace back to original source of attack across stepping stones



Prevalent Approaches

IP Traceback

- Marking (e.g. PPM, DPM)
- Logging

Stepping-stone detection

- Algebraic approach
- Watermarking
- Correlation

Others

- Ingress router filtering/ Back bone router filtering
- Input debugging
- IPSec
- Out-of-band messages (e.g. ICMP)
- Active proving, tracing by hand
- Using IDS, honetpot
- Passive observation
- Social engineering

None of them work for our traceback problem

Grimm's Fairy Tales "Hansel and Gretel"

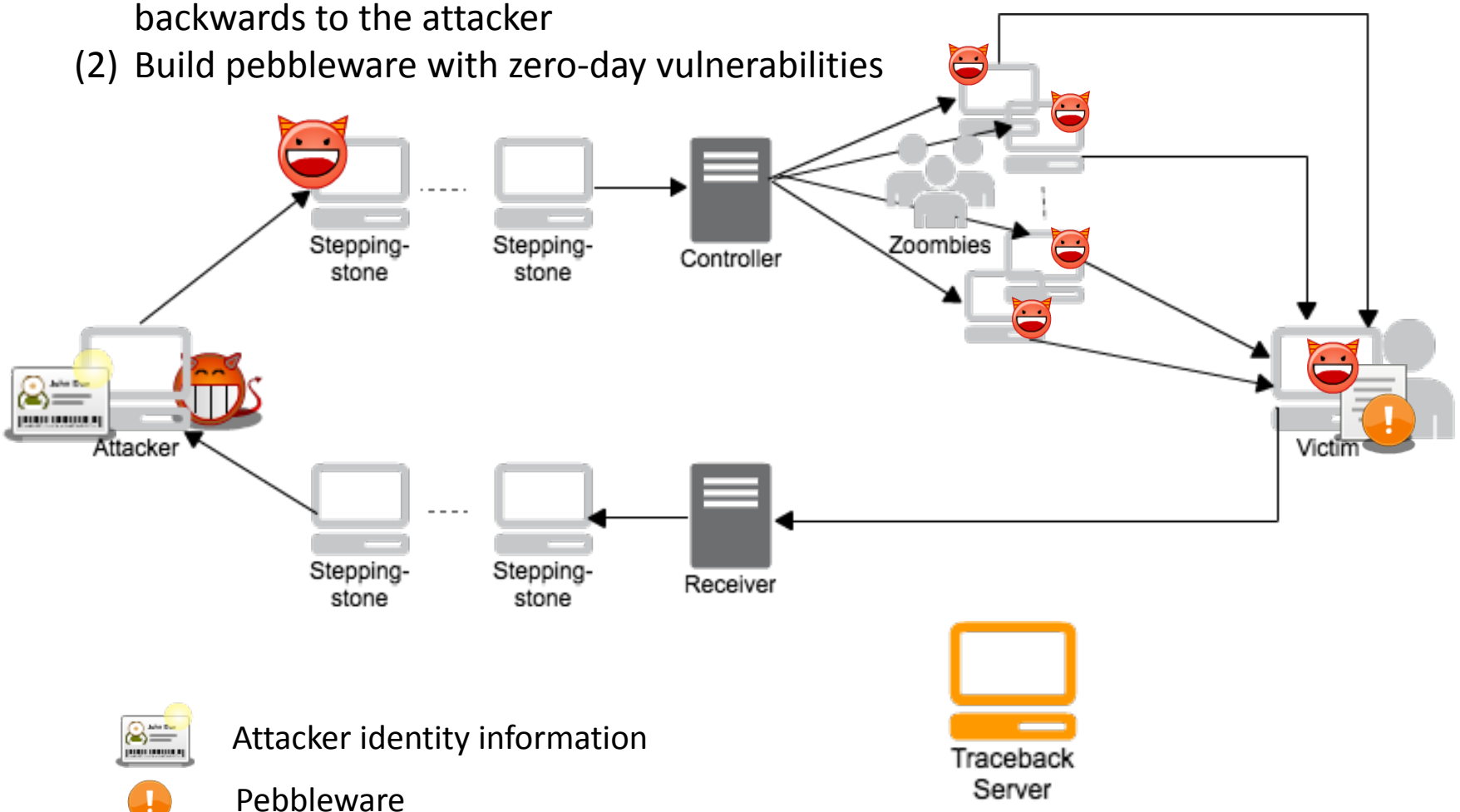
Courtesy by Childrensillustrators

Our Approach: Pebbletrace

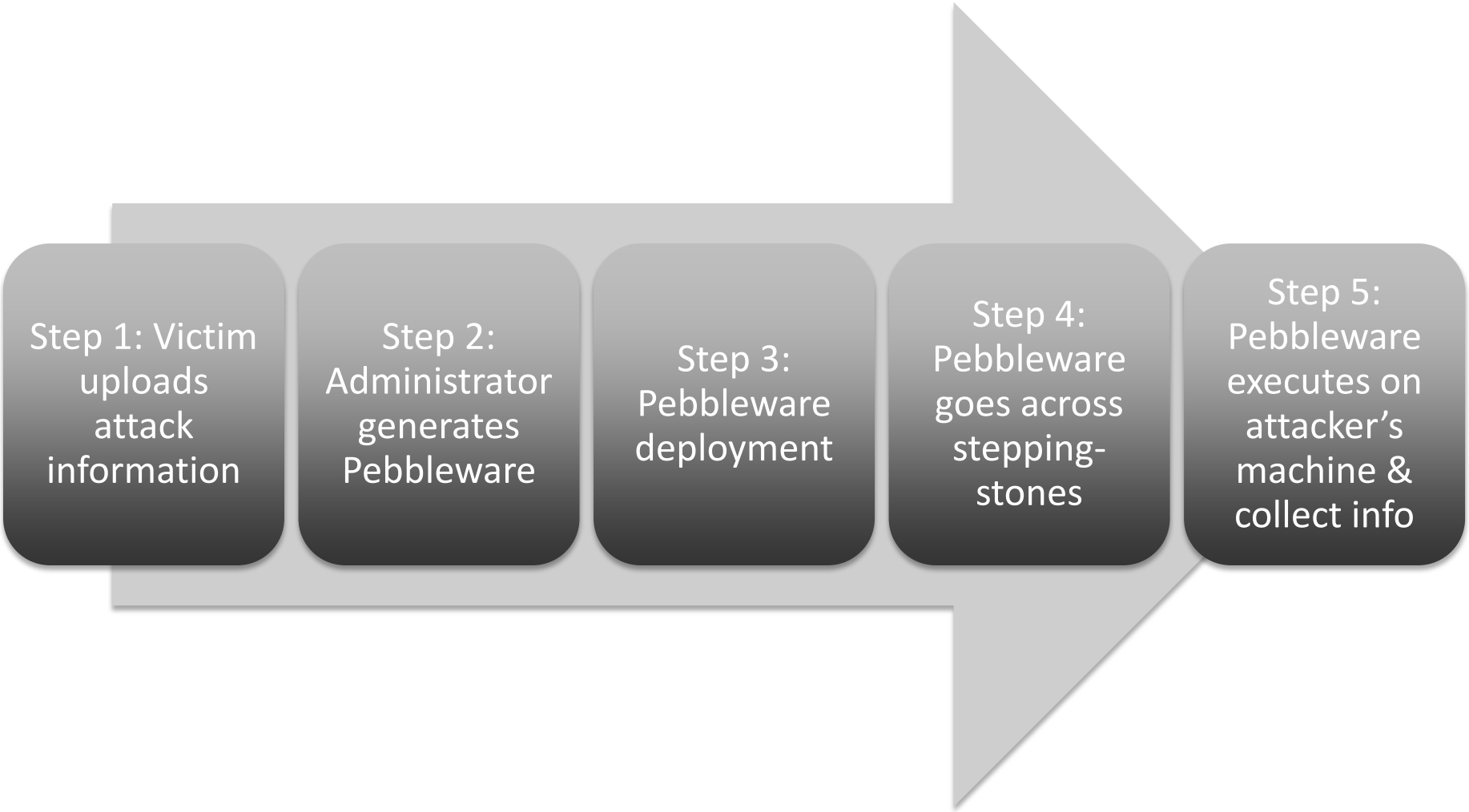
Key idea:

(1) Take advantages of attacking traffic and trace backwards to the attacker

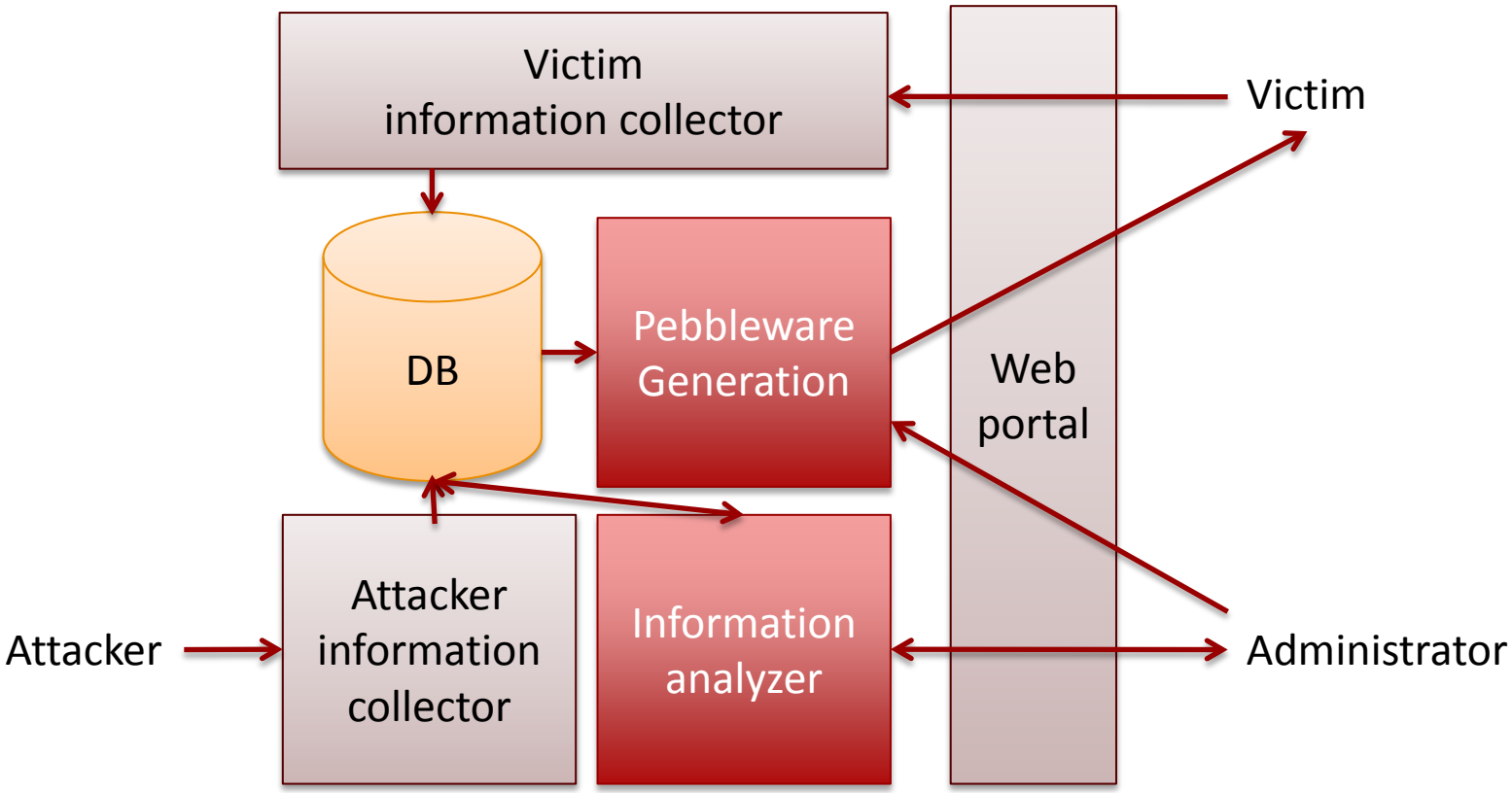
(2) Build pebbleware with zero-day vulnerabilities



Steps of Pebbletrace



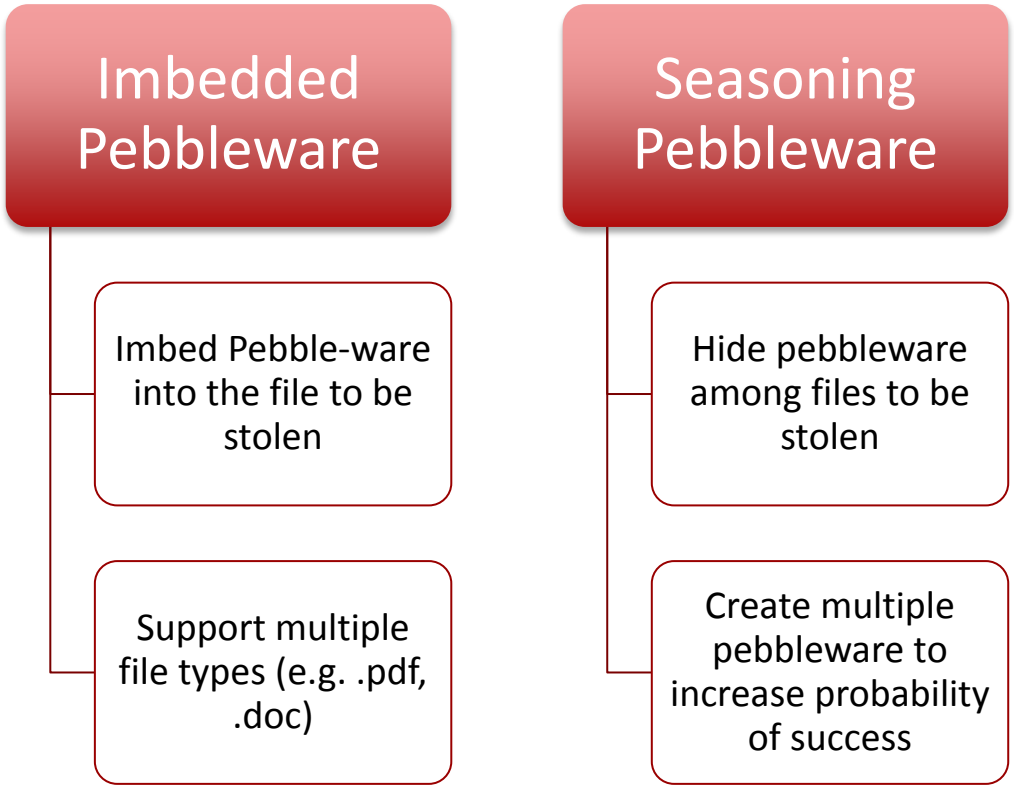
Architecture of Traceback Server



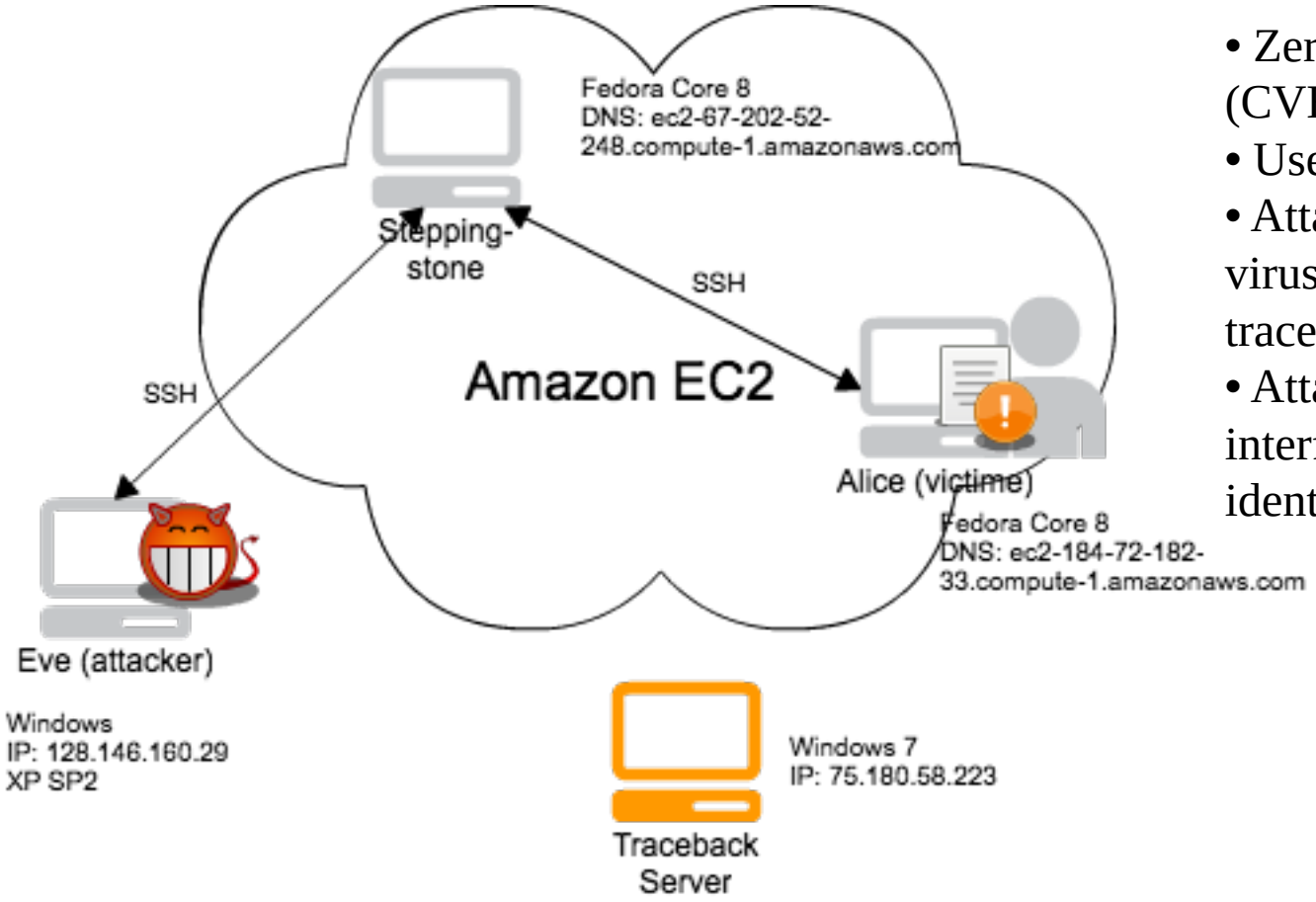
Problem 1: Attacker Steals Files

Key ideas

- Design Pebbleware based on client-side zero-day vulnerabilities
- Traceback attacker once the file containing Pebbleware is opened



Case Study: Traceback File Theft at Amazon EC2



- Zero day: Adobe util.printf() (CVE-2008-2992)
- Use heap spray techinique
- Attacker's firewall and anti-virus tools do not react to the traceback.
- Attacker's IP, network interfaces, snapshot, etc. are identified.

Due to legal issues, the attack in the case study is constructed for study based on possible behaviors of real attackers, not accessible by public.

Problem 2: Attacker Steals Information

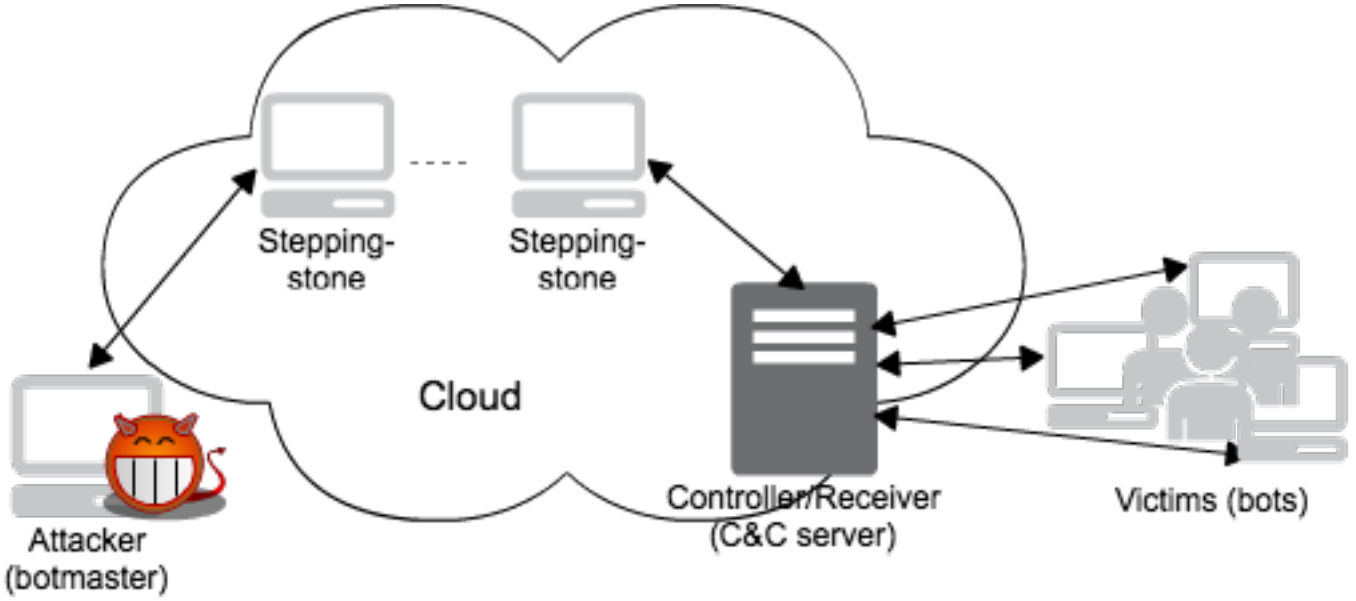
- Attacker steals confidential information (e.g. bank password) directly with hacker tools.
- How to imbed Pebbleware?

Focus on a scenario:

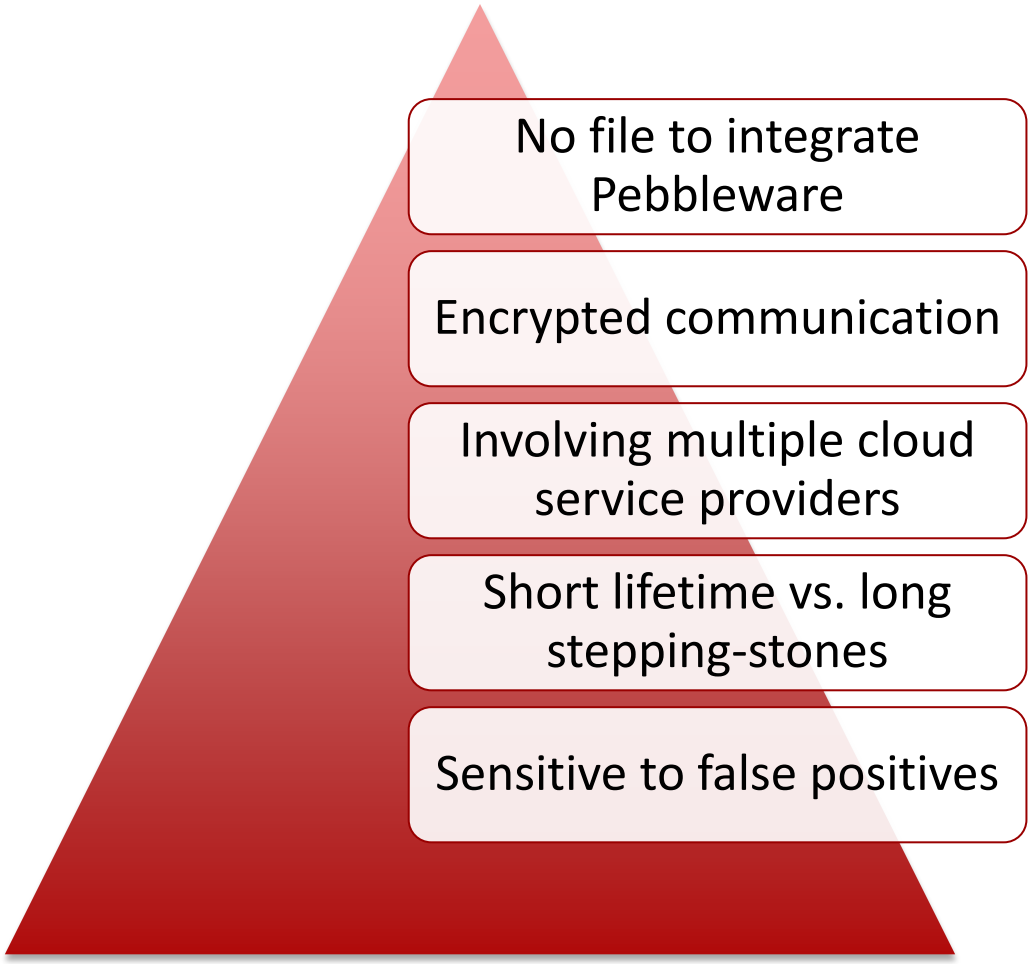
Traceback botmasters in cloud

Botnet Attacks in Cloud

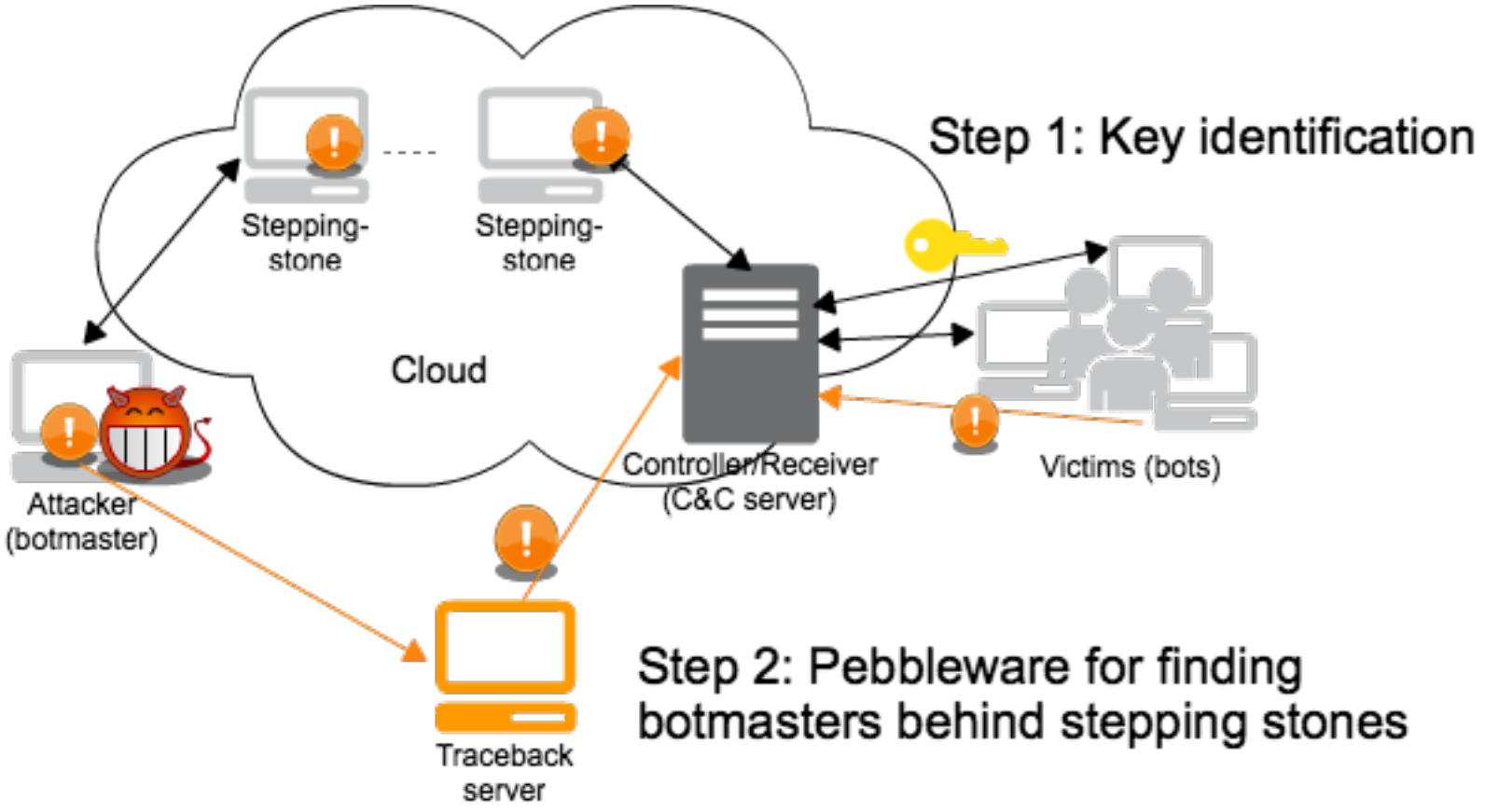
- Scenarios
  - Communicating with victims
  - C&C servers and stepping stones in clouds
  - A centralized C&C server
  - Stepping stones: VPN, proxies and SSH tunneling
  - Symmetric encryption
    - RC4: Zeus, Feederbot; AES: Wraith, Waledac; DES: Ozdok
- Traceback: identify the botmaster behind stepping stones



Extra Challenges



A General Approach to Pebbletracing Botmaster

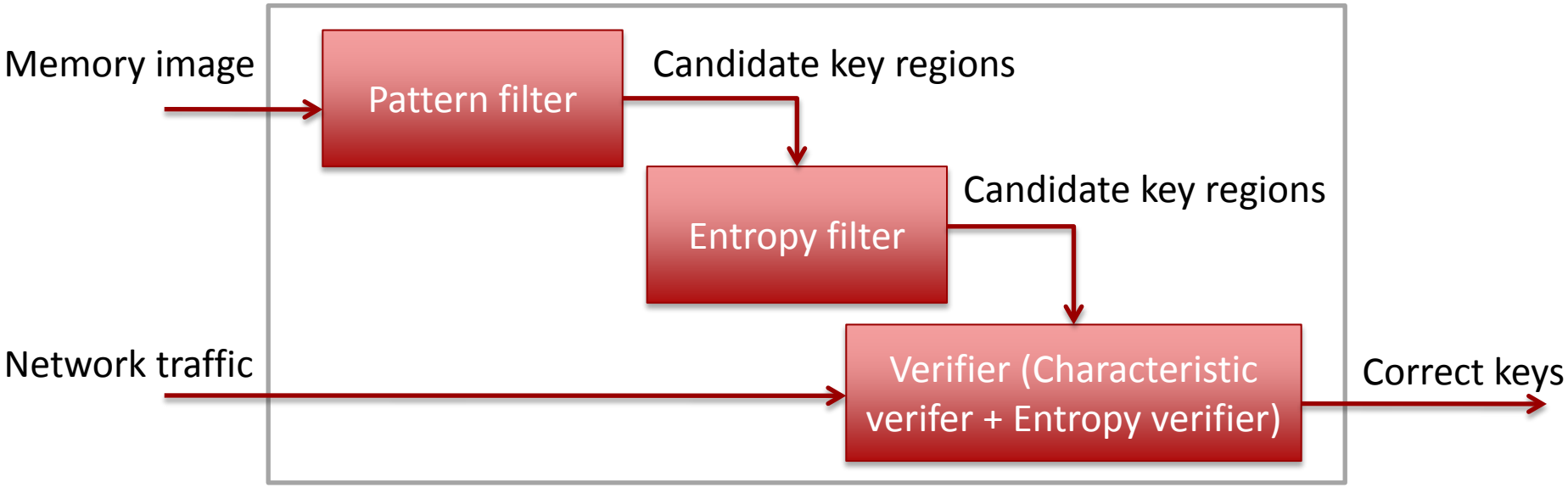


Step 1: Key Identification

- Finding the key given a memory image and encrypted traffic
- Constraints
  - No source code
  - Abnormal format patterns
  - Hard to verify candidate keys
  - Requiring low false positives

A Key Identification Scheme

- Observations
  - Fuzzy delimiter patterns may be available
  - Characteristics of symmetric keys
  - Randomness of ciphertext mostly from symmetric encryption schemes



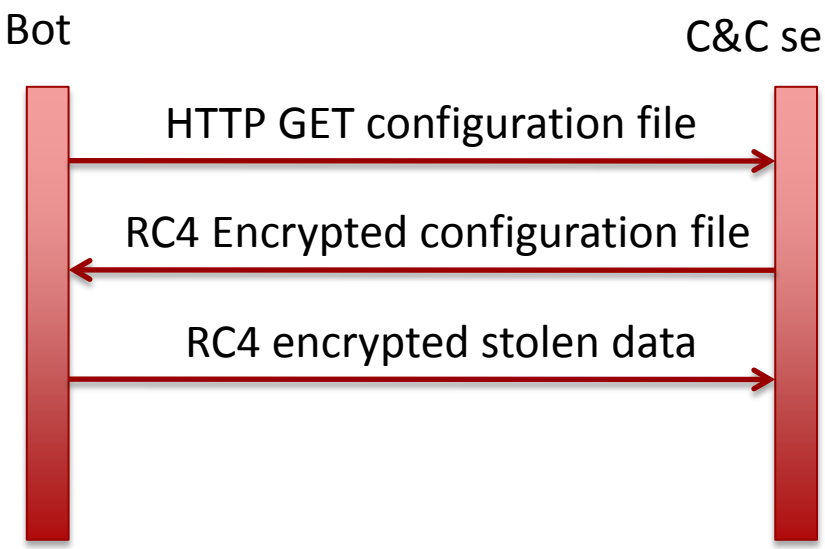
Step 2: Pebbleware for Finding Botmasters

- Exploit zero-day vulnerabilities
  - Vulnerabilities of C&C servers
  - Client-side vulnerabilities
- Hard to select zero-days
- Hide Pebbleware into stealth traffic
  - Option 1: from victim
  - Option 2: from traceback server (e.g. pretend to be a victim)

Case Study: Traceback Zeus Botmaster in Opsource Cloud

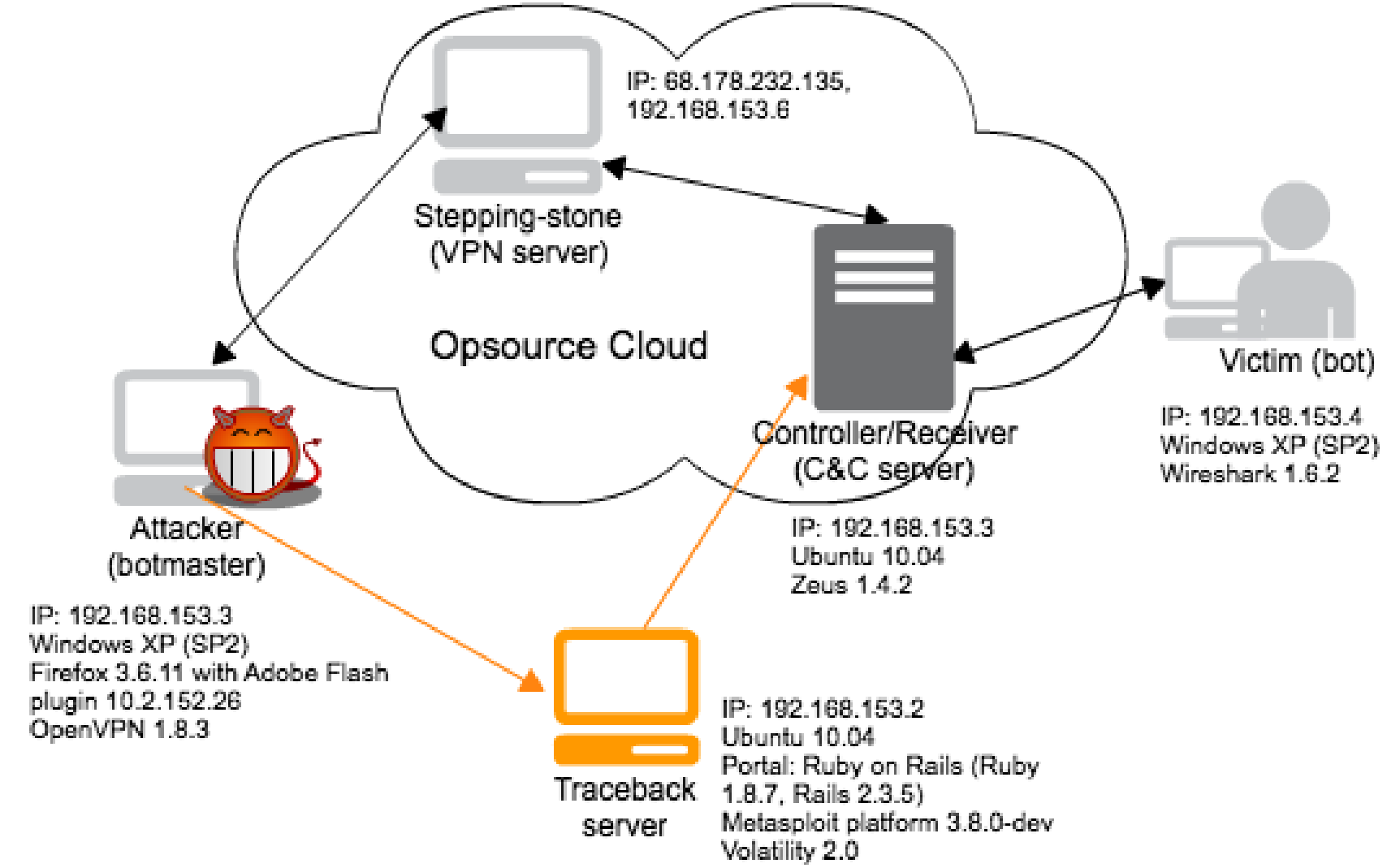
Zeus: The king of bot

Distribution of Zeus C&C servers
(Jun 16, 2012 Courtesy by Zeustracker)



Basic Zeus protocol between bots and C&C server

Case Study: Traceback Zeus Botmaster in Opsource Cloud



Five Steps to Traceback Zeus Botmaster

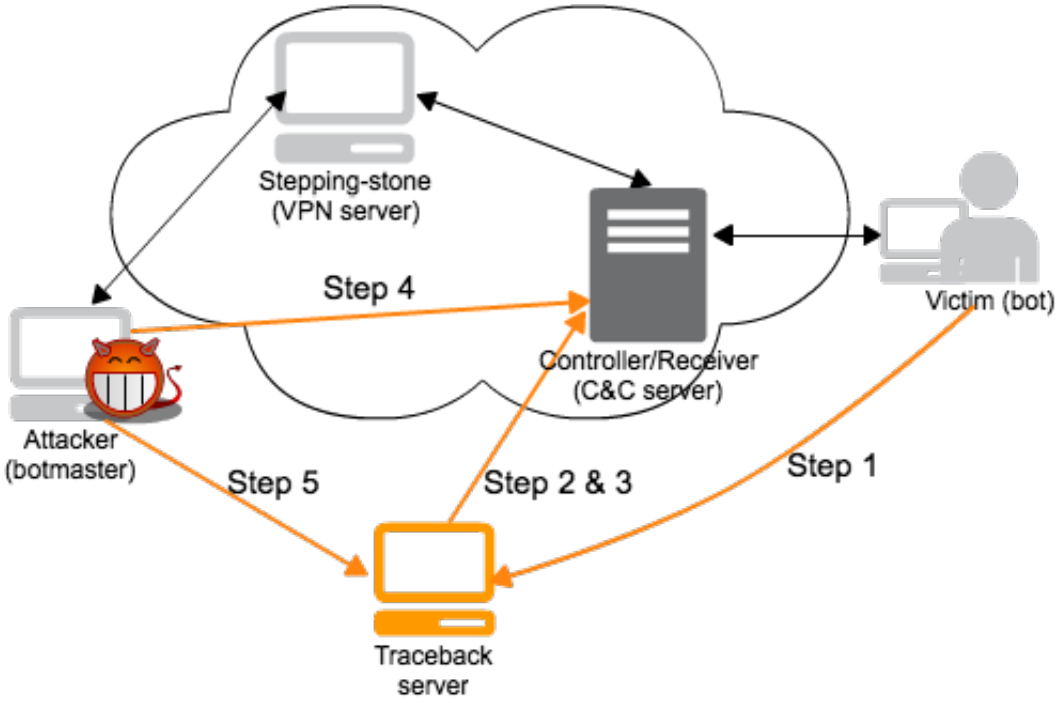
Step 1: Obtaining Information;

Step 2: Pebble 1---uploading the backdoored control panel;

Step 3: Pebble 1'---Replacing the control panel;

Step 4: Botmaster logins to C&C and is logged and redirected;

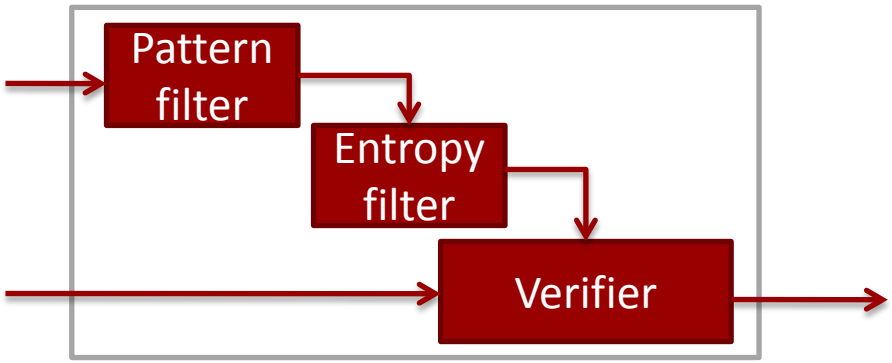
Step 5: Pebble 2---Penetrate stepping-stones collect attacker information.



Step 1: Key Identification of Zeus Botnet

Identify RC4 keys of Zeus Bots

- Pattern filter: 2 zero bytes + 256--400 bytes + 2 zero bytes
- Entropy Analyzer: >7.5
- Verifier
  - Characteristics of key: a permutation of values in 0—255
  - Entropy verifier: the candidate key with largest entropy drop is the real key



Identified key & Decrypted Traffic

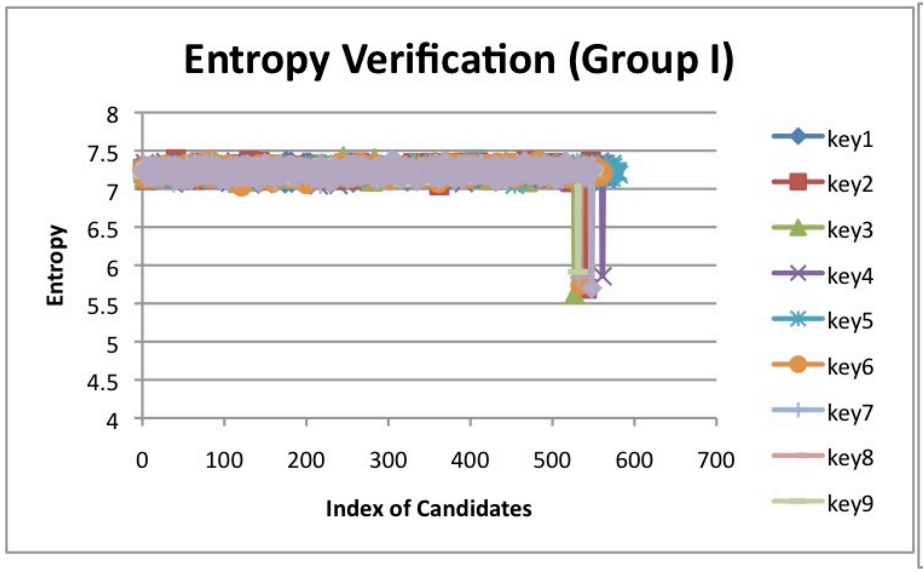
"\004\001\000\000\000\000\000\000\n\000\000\000:\340\350y\323\235\364\264\360x_y\326\225O\226\021'\000\000\000\000\000\000\030\000\000\000\030\000\000\000winxp_803cde68e_001938c9\023'\000\000\000\000\000\000\004\000\000\000\004\000\000\000\001\n\002\001\031'\000\000\000\000\000\000\004\000\000\000\004\000\000\000\336u4N\e'\000\000\000\000\000\000\004\000\000\000\004\000\000\000\300\307\377\377\032'\000\000\000\000\000\000\004\000\000\000\004\000\000\000\"?\031\000\034'\000\000\000\000\000\000\024\000\000\000\024\000\000\000\005\000\000\000\001\000\000\000{\n\000\000\002\000\000\000\000\001\001\000\035'\000\000\000\000\000\000\002\000\000\000\002\000\000\000\t\004\024'\000\000\000\000\000\000\004\000\000\000\004\000\000\000e\000\000\000\025'\000\000\000\000\000\000\004\000\000\000\004\000\000\000\000\000\000\000\026'\000\000\000\000\000\000\002\000\000\000\002\000\000\000\000\000"

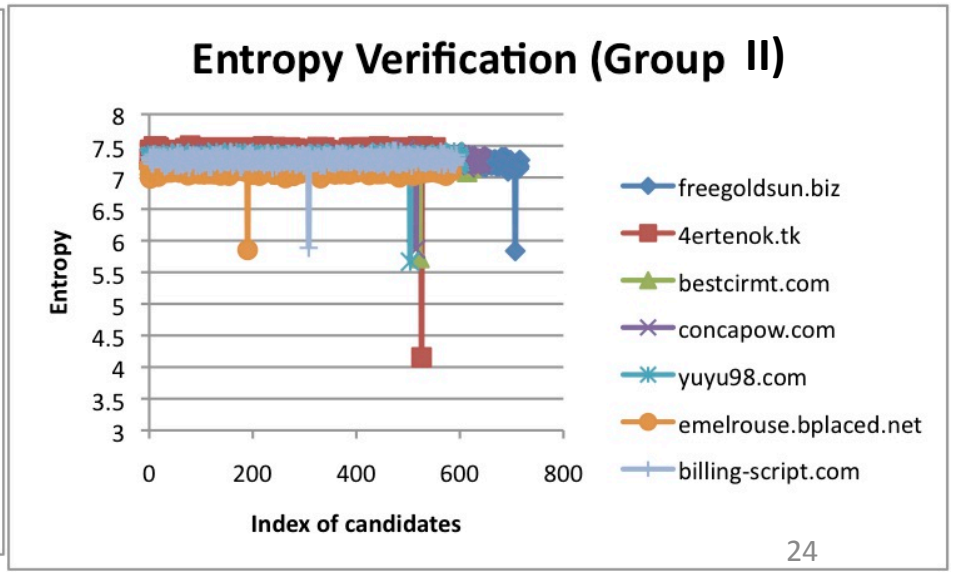
A detected S table of a Zeus bot

A decrypted traffic of a Zeus bot

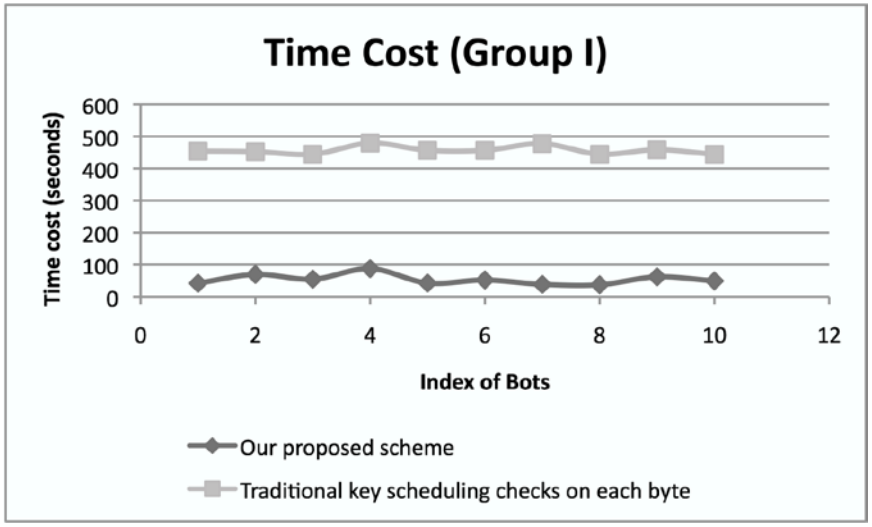
Performance of Entropy Verifier

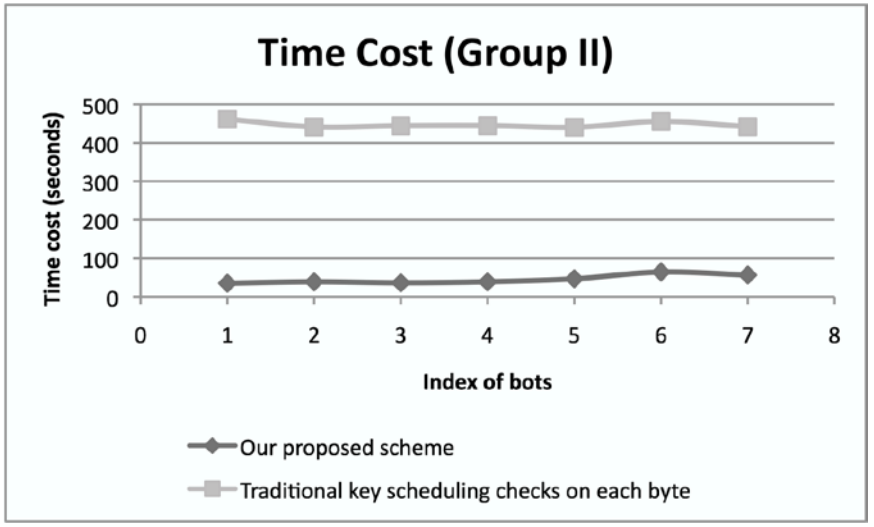
- Two groups of bots
  - I. Homegrown
  - II. Wild caught
- Outliers: the correct keys

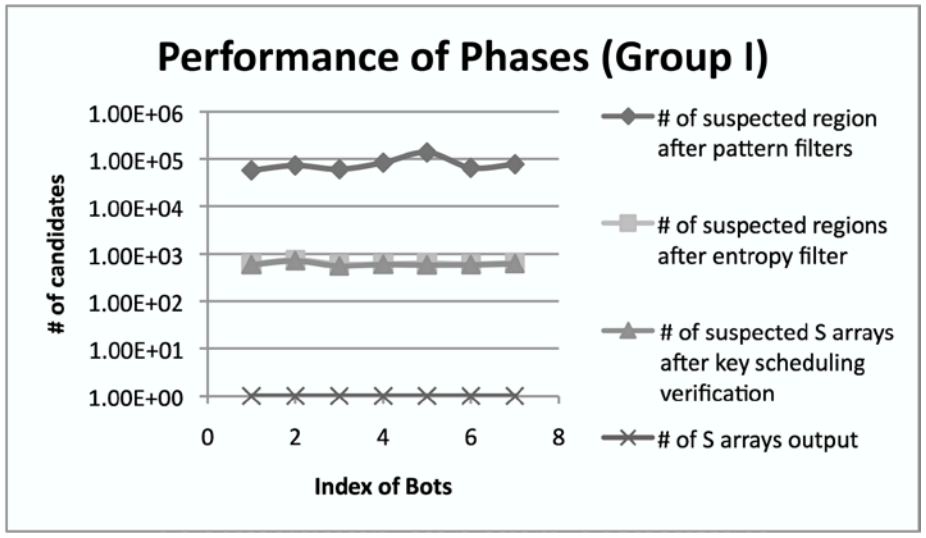


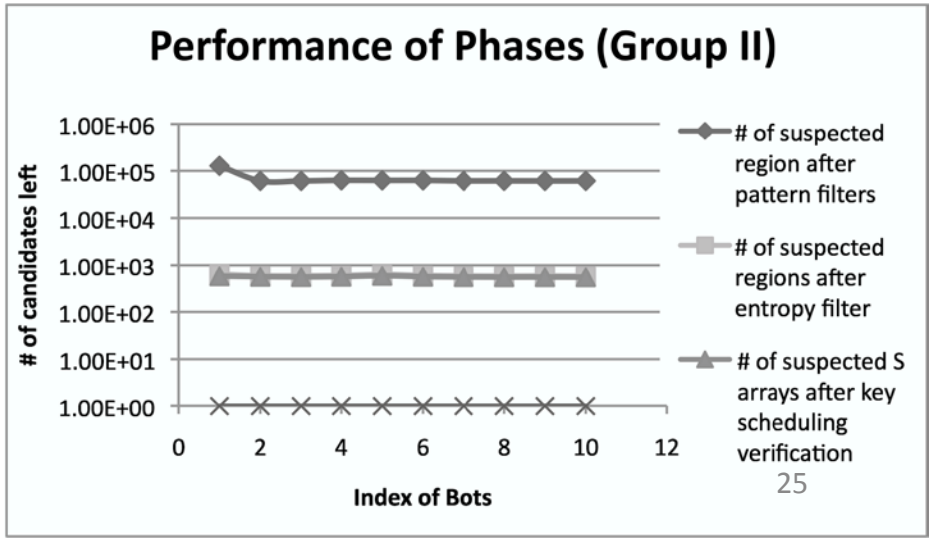


Performance of the Key Identification Scheme in Zeus Botnets

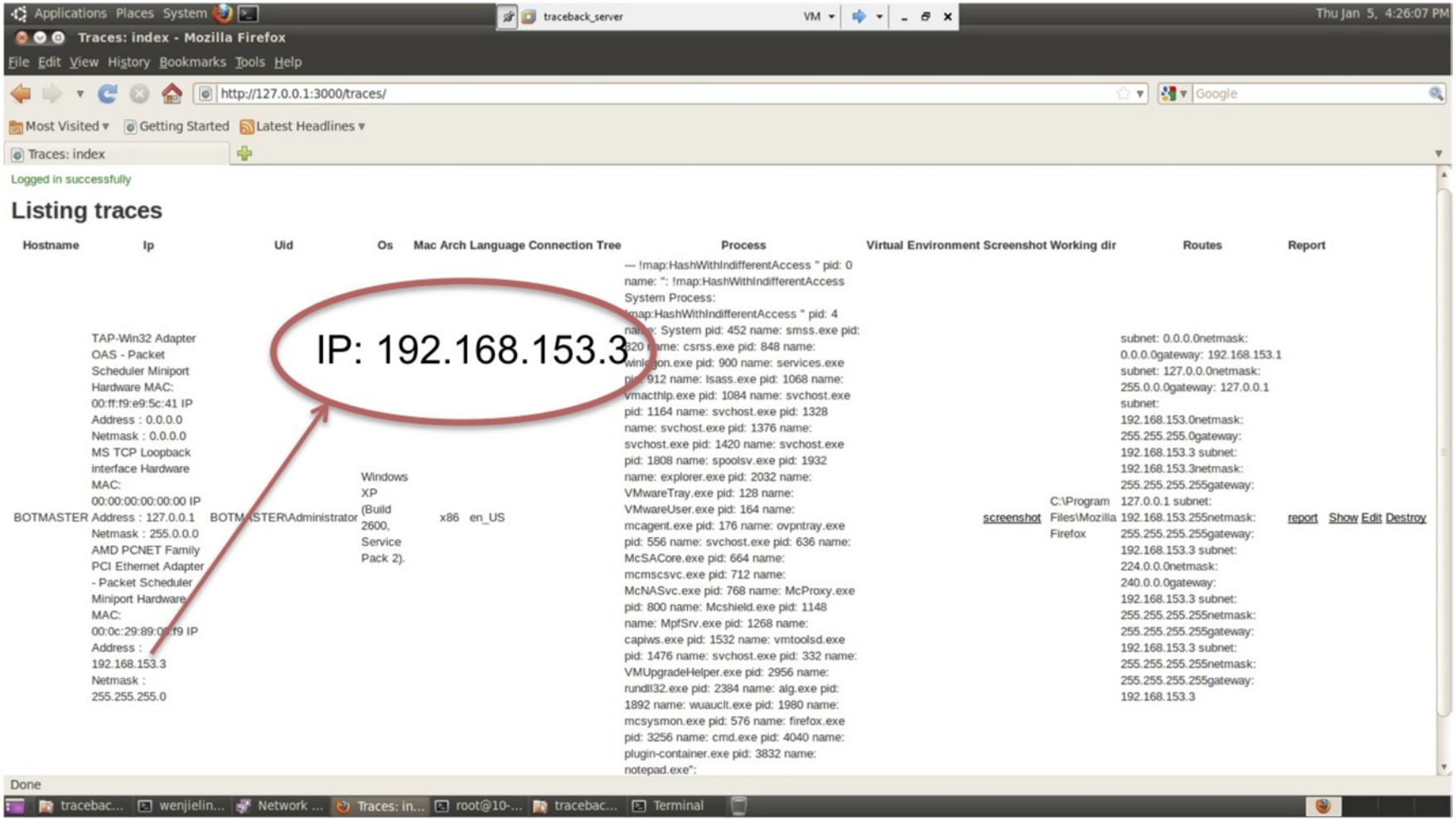








Attacker Information Detected



Conclusion

- Traceback Internet attacks
  - Attacker steals files
  - Attacker steals information
    - Traceback botmaster in clouds
- Future work
  - Attacker communicates with victims through social networks

Publications

- W. Lin and D. Lee, Traceback Attacks in Cloud— Pebbletrace Botnet, IEEE ICDCS SPCC, 2012
- Y. Hsu and D. Lee, Machine Learning for Implanted Malicious Code Detection with Incompletely Specified System Implementations, IEEE ICNP FIST, 2011
- G. Shu and D. Lee, "A Formal Methodology for Network Protocol Fingerprinting", IEEE Trans on Parallel and Distributed Systems, 2011
- Z. Liu, G. Shu and D. Lee, Instant Messaging Security, in Network Security, Administration and Management: Advancing Technologies and Practices, D. C. Kar and M. R. Syed, ed., IGI Global, 2010
- F. Yu, V. Gopalakrishnan, K. K. Ramakrishnan and D. Lee, “Loss-tolerant Real-time Content Integrity Validation for P2P Video Streaming”, COMSNETS 2009
- F. Yu and D. Lee, "Internet Attack Traceback - Cross-validation and Pebble Tracing", IEEE/DHS International Conference on Technologies for Homeland Security, May 2008
- Y. Hsu, G. Shu and D. Lee, “A Model-based Approach to Security Flaw Detection of Network Protocol Implementations”, IEEE ICNP Oct 2008
- G. Shu, Y. Hsu and D. Lee, “Fuzz Testing and Communications Protocol Security Flaws”, June FORTE 2008
- G. Shu, D. Chen, Z. Liu, N. Li, L. Sang and D. Lee, “VCSTC: Virtual Cyber Security Testing Capability – An Application Oriented Paradigm for Network Infrastructure Protection”, TESTCOM/FATES June 2008
- P. Pederson, D. Lee, G.-Q. Shu, D. Chen, Z. Liu, N. Li and L. Sang, "Virtual Cyber-Security Testing Capability for Large Scale Distributed Information Infrastructure Protection", IEEE/DHS International Conference on Technologies for Homeland Security, May 2008

Reference

[1] Sony Attacked Again, Passwords and Other Data Stolen http://threatpost.com/en_us/blogs/sony-attacked-again-passwords-and-other-data-stolen-060311.

[2] Paris G20 files stolen in cyber attack http://www.homelandsecuritynewswire.com/paris-g20-files-stolen-cyber-attack.

[3] Hacked: Data breach costly for Ohio State, victims of compromised info
http://www.thelantern.com/campus/hacked-data-breach-costly-for-ohio-state-victims-of-compromised-info-1.1831311.

[4] S. C. Lee and C. Shields, "Tracing the Source of Network Attack: A Technical, Legal and Societal Problem", In *Proc. of the 2001 IEEE Workshop on Information Assurance and Security*, June 2001.

[5] Guang Yao, Jun Bi, Zijian Zhou, "Passive IP traceback: capturing the origin of anonymous traffic through network telescopes", Proceedings of the ACM SIGCOMM 2010.

[6] Zeus (trojan horse), http://en.wikipedia.org/wiki/Zeus_(trojan_horse).

[7] Zeus: King of the Bots, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf.

[8] Zeus Tracker, https://zeustracker.abuse.ch/.

[9] John the Ripper password cracker, http://www.openwall.com/john/.

[10] Taking over Zeus Botnet, http://xs-sniper.com/sniperscope/Zeus/CnC-Pwn-with-dir-traversal.txt

[11] Zeus botnets' Achilles' Heel makes infiltration easy, http://www.theregister.co.uk/2010/09/27/zeus_botnet_hijacking/.

[12] Metasploit, http://www.metasploit.com/.

[13] Metasploit PHP Executable Download and Execute payload, http://www.metasploit.com/modules/payload/php/download_exec.

[14] CVE-2011-0609, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609

[15] RC4 http://en.wikipedia.org/wiki/RC4

[16] Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., Wang, L., On the analysis of the Zeus botnet crimeware toolkit, Privacy Security and Trust (PST), 2010

[17] Adi Shamir and Nicko van Someren, Playing hide and seek with stored keys, Lecture Notes in Computer Science, 1999, Volume 1648/1999, 118-124