Botconf 2013

Éric Freyssinet – Afterwork OSSIR 28/01/2014

Plan

- Pourquoi une conférence sur les *botnets*?
- L'équipe d'organisation et le comité de programme
- Calendrier
- Contenu scientifique
- Et après?

Pourquoi une conférence sur les botnets? (1/2)

- Définition proposée dans l'appel à communications:
  - Botnets: "The term botnets is used to define networks of infected end-hosts, called bots, that are under the control of a human operator commonly known as the botmaster. While botnets recruit vulnerable machines using methods also utilized by other classes of malware (e.g., remotely exploiting software vulnerabilities, social engineering, etc.), their defining characteristic is the use of command and control (C&C) channels to connect bots to their botmasters." (A multifaceted approach to understanding the botnet phenomenon, Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas Terzis, in Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (IMC '06))

Pourquoi une conférence sur les botnets? (2/2)

- Sujet abordé uniquement dans des conférences fermées, ou de façon accessoire et peu visible (conférences discrètes sur les virus)
- Ou alors abordé au cours des conférences de sécurité classiques, parmi un nombre important d'autres sujets, sans que les spécialistes de la question soient forcément présents
- C'est un domaine suffisant large pour justifier d'une véritable conférence, et en plus on peut enfin l'aborder sous un angle pluridisciplinaire (y compris juridique, social, comportemental, etc…)

L’équipe d’organisation

- Equipe d’organisation française, constituée en association:
  - Frédéric Le Bastard
  - Cédric Le Roux
  - Paul Rascagnères
  - Samir Bellabes
  - Erwan Abgrall
  - Steeve Barbeau
  - Eric Freyssinet
  - Reza Elgalai
  - Frédéric Baguelin
  - Sébastien Larinier
  - Jean-Philippe Teissier
  - Fabien Duchêne
- Nous ont rejoint:
  - Geoffroy Couprie
  - Paul Dozancuk

Le comité de programme, international et indépendant

- Hendrik Adrian, CEO, KK KLJTECH, Tokyo, Japan
- José Araujo, Deputy Head of the Applied and Fundamental Research Division, French Network and Information Security Agency (ANSSI), France
- Domagoj Babic, Research Scientist, Facebook, Inc., United States of America
- Gilles Berger-Sabbatel, Chargé de recherches, CNRS, Laboratoire d'Informatique de Grenoble, France
- Guillaume Bonfante, Assistant-Professor, Lorraine University, France
- Nicolas Brulez, Malware expert, Kaspersky Lab, France
- Alexandre Dulaunoy, Security Researcher, CIRCL, Computer Incident Response Center Luxembourg, National CERT, Luxembourg
- Barry Irwin, Associate Professor, Rhodes University, Computer Science, South Africa
- Denis Laskov, Independent researcher, Israël
- Corrado Leita, Principal research engineer, Symantec, France
- Jean-Yves Marion, Professor, LORIA, Université de Lorraine, France
- David Naccache, Ecole Normale Supérieure, France
- Fred Raynal, CEO, Quarkslab, France

Calendrier

- Novembre 2012: création de l'association et constitution du comité de programme
  - Pendant cette période, identification du lieu et des sponsors
- Février 2013: lancement du CFP
- 30 Juin 2013: première deadline et lancement du second CFP (short papers/presentations)
- Septembre 2013: annonce du programme
- 5 et 6 décembre 2013: déroulement de la conférence à Nantes
- Ensuite: sondage, paiement des factures, etc…

Contenu scientifique (1/5)

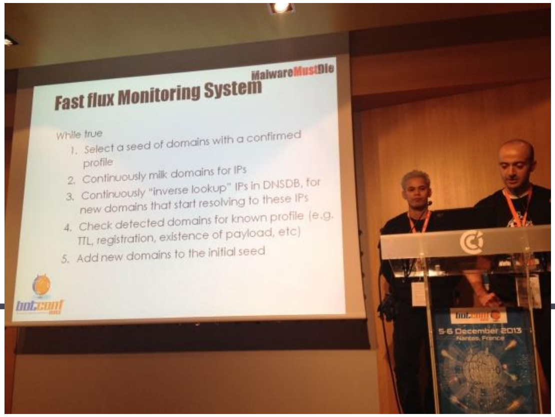
- https://www.botconf.eu/index.php/schedule/
  - 25 sessions dont 7 short talks et 4 papers
  - 1 – ACDC http://www.botfree.eu
  - 2 – Advanced techniques in modern banking trojans (Thomas Siebert, GData, Allemagne)
  - 3 – Spam and all things salty: Spambot v2013 (Jessa dela Torre, Trend Micro, Philippines)
  - 4 – Distributed Malware Proxy Networks (Brad Porter, Nick Summerlin)
  - 5ST – Legal limits of proactive actions: Coreflood botnet example (Oguz Kaan Pehlivan, Turquie)

Contenu scientifique (2/5)

- 6ST – *Back to life, back to correlation* (Vasileios Friligkos, Intrinsec, France)
- 7ST - *Using cyber intelligence to detect and localize botnets* (Enrico Branca, France)
- 8 – *Zombies in your browser* (Prakhar Prasad and Himanshu Sharma, Inde)
- 9 – *Spatial Statistics as a Metric for Detecting Botnet C2 Servers* (Etienne Stalmans and Barry Irwin,Afrique du Sud)
- 10 – *The Home and CDorked campaigns :Widespread Malicious Modification ofWebservers for Mass Malware Distribution* (Sébastien Duquette, ESET, Canada)

Contenu scientifique (3/5)

- 11ST – *Malware Calling* (Maciej Kotowicz)
  - https://github.com/mak/random-stuff/tree/master/powerzeus
- 12ST – *Disass* (Ivan Fontarensky, Cassidian, France)
  - http://bitbucket.cassidiancybersecurity.com/disass
  - “Disass is a binary analysis framework written in Python to ease the automation of static malware reverse engineering. The purpose of Disass is to automatically retrieve relevant information in a malware such as the C&C, the user agent, cipher keys, etc.”
- 13ST – *Efficient Program Exploration by Input Fuzzing* (Thanh Dinh Ta, Inria, France)
- 14ST – *The power of a team work – Management of Dissecting a Fast Flux Botnet, OP-Kelihos “Unleashed”* (Hendrik Adrian and Dhia Mahjoub)



MalwareMustDie

Fast flux Monitoring System

```
While true
    1. Select a seed of domains with a confirmed
       profile
    2. Continuously milk domains for IPs
    3. Continuously "inverse lookup" IPs in DNSDB, for
       new domains that start resolving to these IPs
    4. Check detected domains for known profile (e.g.
       TTL, registration, existence of payload, etc)
    5. Add new domains to the initial seed
```

Contenu scientifique (4/5)

- 15 – Perdix: a framework for realtime behavioral evaluation of security threats in cloud computing environment (Julien Lavesque, Itrust France)
- 16 – *Participatory Honeypots: A Paradigm Shift in the Fight Against Mobile Botnets* (Pasquale Stirparo, JRC Ispra, Italie)
- 17 – *My Name is Hunter, Ponmocup Hunter* (Tom Ueltschi, Suisse)
- 18 – *Reputation-based Life-course Trajectories of Illicit Forum Members* (David Décary-Hétu, Suisse/Canada)
- 19 – *APT1: Technical Backstage* (Paul Rascagnères, France/Luxembourg)

Contenu scientifique (5/5)

- 20 – *Invited talk: Europol and European law enforcement action against botnets* (Jaap van Oss, Europol)
- 21 – *A General-purpose Laboratory for Large-scale Botnet Experiments* (Thomas Barabosch, Univ. Bonn, Allemagne…)
- 22 – *DNS Resolution Traffic Analysis Applied to Bot Detection* (Ronan Mouchoux)
- 23 – *Exploit Krawler: New Weapon againt Exploits Kits* (Sébastien Larinier, Guillaume Arcas, Sekoia, France)
- 24 – *BladeRunner: Adventures in Tracking Botnets* (Jason Jones, Marc Eisenbarth)
- 25 – *The hunter becomes the hunted – analyzing network traffic to track down botnets* (Thomas Chopitea)
  - https://github.com/tomchop/malcom

Compte-rendus en ligne

- http://blog.rootshell.be/2013/12/06/botconf-2013-wrap-up-day-1/
- http://blog.rootshell.be/2013/12/07/botconf-2013-wrap-up-day-2/
- http://www.virusbtn.com/blog/2013/12_10.xml
- http://www.lexsi-leblog.fr/cert/botconf-la-sweet-orange-conference.html
- http://bl0g.cedricpernet.net/post/2013/12/12/Botconf-2013-A-real-success
- http://labs.umbrella.com/2013/12/18/operation-kelihos-presented-botconf-2013/
- …

Les vidéos sont en ligne !

- … On commence à les mettre en ligne progressivement (une dizaine seront disponibles ce soir)
- Streaming pendant la conférence et gros travail d'édition après par Frédéric Baguelin

Et maintenant

- Nous avons une belle communauté française capable de travailler sur la lutte contre les botnets, on va donc continuer !
- On est repartis pour 2015
  - Nancy
  - Première semaine de décembre
  - Pendant 3 jours a priori
  - Dans les locaux du LORIA
  - https://www.botconf.eu @Botconf
- Objectifs: des sujets plus variés (droit notamment) et plus d'implication policière européenne