C&ESAR 2020 - Leurrage numérique

appel à communications

17 – 18 Novembre 2020 – Rennes - France

Computer & Electronics Security Applications Rendez-vous

www.cesar-conference.fr

À propos de C&ESAR

Le Ministère des Armées organise depuis 1997 la conférence C&ESAR dédiée à la cybersécurité. Elle réunit les acteurs gouvernementaux, industriels et académiques dans une approche interdisciplinaire, permettant aux industriels et aux scientifiques de confronter la recherche et le développement aux réalités opérationnelles et aux utilisateurs d'étudier et d'anticiper les avancées technologiques. La conférence se déroule dans le cadre de la European Cyber Week (ECW).

Leurrage numérique *(Deceptive security)*

La cybersécurité s'est développée depuis une quinzaine d'années en réponse à l'agressivité croissante des attaques informatiques. L'essor du cyberespace est inhérent à l'explosion des besoins de services et de communications et donc de débits et de nouvelles technologies. Construit sur une base pragmatique pour offrir rapidement de nouveaux produits, le cyberespace a atteint un niveau de complexité difficilement maîtrisable. Cette situation a donné un avantage prépondérant aux attaquants qui ont su transformer une imperfection en faille puis en scénarios d'attaque pour des finalités hostiles. La réponse de la sécurité informatique a entre-temps évolué d'une protection statique en profondeur, vers une détection résiliente pour désormais envisager des logiques de contre-attaques dynamiques. L'échelle de temps entre l'occurrence d'une attaque, sa détection et son élimination est un marquant significatif: d'une durée indéterminée à quelques jours, puis de jours à quelques heures, l'enjeu est maintenant d'agir en temps réel contre l'attaquant. Le leurrage numérique se trouve au cœur de cette stratégie de la cybersécurité. Il s'agit de retourner les armes de l'attaquant en cherchant à le tromper et au final à le dissuader de prendre le risque d'être découvert. Le leurrage numérique relève de la dissuasion cyber.

L'arsenal du leurrage défensif est historiquement basé sur les pots de miel (*honeypots*). Ceux-ci reposaient sur l'analyse statique d'écart de composants par rapport à un comportement connu et sain. Cette génération s'est heurtée à deux écueils : le passage à l'échelle pour couvrir la diversité et la complexité des systèmes numériques, et la génération excessive de faux positifs. Les honeypots évoluent pour devenir des pièges actifs qui sont disséminés dans l'environnement réel pour mieux cerner les stratégies de l'attaquant. Les architectures de déploiement des leurres se spécialisent selon le domaine d'application (systèmes d'information, systèmes industriels, finance, médical...) ou en fonction des composants ciblés par les attaques (serveurs, pare-feu, antivirus...) ou encore par rapport à la charge offensive (malwares...). Les leurres tendent à générer de vrais positifs en temps réel. Leur efficacité repose sur deux propriétés, l'une inhérente aux composants de sécurité, la non-compromission, et l'autre caractéristique de l'attaque : la furtivité.
Cette nouvelle génération de leurres numériques enrichit les stratégies d'investigations au sein des centres opérationnels de sécurité (SOC). Ainsi, des logiques de raisonnements déductifs (déterministes) ou inductifs (hypothétiques) se confrontent pour caractériser finement le mode opératoire des attaquants en le resserrant si possible jusqu'à l'attribution de l'attaque.
Cependant, son caractère actif soulève des interrogations réglementaires (respect de la vie privée).
Le leurrage numérique devient une composante essentielle de la lutte informatique défensive, car il contribue à l'efficience des scénarios de ripostes et d'escalade.

Le comité de programme de la conférence C&ESAR 2020 attend des propositions de communication en matière de recherche, d'expérimentation et de solutions émergentes sur :

- Leurrage numérique : honeypots, leurres, pièges
- Architectures de déploiement de leurres selon les domaines d'application
- Spécialisation de leurres pour les services, pour la sécurité, contre les malwares...
- Propriétés du leurrage numérique : non-compromission, furtivité...
- Apport à l'investigation numérique : raisonnements déductifs/inductifs, caractérisation des attaques, attribution...
- Contribution à la lutte informatique défensive : scénarios de ripostes et d'escalade.
- Positionnement du leurrage dans les modèles d'attaques (MITRE ATT@CK...), par rapport à la caractérisation des attaques (CAPEC...) et plus généralement son apport à la connaissance du risque cyber (cyber threat intelligence – CTI)
- Leurrage et réglementation (NIS, RGPD...).

Modalités de soumission

- *Première étape :* les propositions de communication (3 à 6 pages) sont à soumettre au plus tard le **30 juin 2020 (nouvelle date)** via https://easychair.org/conferences/?conf=cesar2020 , au format PDF. Doivent y figurer le titre de la communication, les noms et prénoms des auteurs ainsi que leur affiliation, l'adresse électronique de l'auteur principal, un résumé (10 lignes max.) et une liste de mots clés. Les auteurs seront prévenus de l'acceptation ou du rejet le **3 septembre 2020**.
- *Seconde étape :* les auteurs envoient au plus tard le **2 octobre 2020** une version définitive de la communication (de 8 à 16 pages) à contact@cesar-conference.org, copie à benoit-f.martin@intradef.gouv.fr. Les auteurs s'engagent dans cette version définitive à prendre en compte les remarques des relecteurs transmises lors de la notification de la décision.
- *Instructions pour la version définitive de l'article* : document PDF au format A4 sans les numéros de page, suivant le modèle Springer Lecture Notes in Computer Science :
  modèle LaTeX : ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip;
  modèle Word : ftp://ftp.springernature.com/cs-proceeding/llncs/word/splnproc1703.zip.
- *Langues et critères de sélection :* les communications peuvent être rédigées en français ou en anglais. Les critères de sélection seront principalement le respect du thème de la conférence et de l'appel à communications, la clarté et l'effort pédagogique. Les exposés techniques seront considérés dans la mesure où ils présentent aussi un état de l'art d'un domaine et non uniquement un résultat particulier. Les communications ne doivent pas être à vocation commerciale. Les communications acceptées seront publiées dans les actes de la conférence consultables sur le site C&ESAR 2020.

Dates importantes

- Soumission des propositions de communications (entre 3 et 6 pages) : **30 juin 2020 (nouvelle date)**
- Notification aux auteurs : **3 septembre 2020**.
- Version finale (entre 8 et 16 pages) : **2 octobre 2020**
- Conférence : **17 et 18 novembre 2020**

Comité de programme

Erwan ABGRALL (MINARM)
Christophe BIDAN (CentraleSupélec)
Frédéric CUPPENS (Polytechnique Montreal)
Eric DUPUIS (Orange)
Ivan FONTARENSKY (THALES)
Sylvain LAFARGUE (SAFRAN)
Guillaume MEIER (AIRBUS)
Ludovic PIETRE-CAMBACEDES (EDF)
Eric WIATROWSKI (Orange)
José ARAUJO (ANSSI)
Yves CORREC (ARCSI)
Herve DEBAR (Télécom SudParis)
Guillaume DUVEAU (MINARM)
Patrick HEBRARD (NAVAL Group)
Benoît MARTIN (DGA)
Marc-Oliver PAHL (IMT Atlantique)
Assia TRIA (CEA)

Partenaires