Feed back - Cyb’Air Sud 2025

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

ÉCOLE DE L'AIR ET DE L'ESPACE - BASE AÉRIENNE 701 - SALON-DE-PROVENCE

PROGRAMME

Heure	Durée	Salle MLM	Salle DELAVAL
8:30	20'	Accueil - café	
9:00	30	OUVERTURE	
9:40	30'	Trust Me, I'm a Shortcut: New LNK Abuse Methods Wietze beukema	
10:20	30'	Analyse de malware avec r2ai et mcp Axelle Apvrille	The Kill Chain for Android Malware: Delivery Thibaud P.
11:00	30'	Vshell: The V stands for Verbose Maxime Thiebaut	Détection Comportementale des Activités sur Disque des Ransomwares et Génération de Données Synthétiques pour Anticiper les Attaques Futures Damien Lescos
11:40 - 14:00	140'	MEET UP & REPAS	
14:00	30'	Du SOC au CERT : ce que le reverse engineering de malwares apporte vraiment Hugo RIFFLET	Malware craftsmanship Sonia Seddiki
14:40	30'	Malware Operations Under the Microscope: From Binary Artifacts to Strategic Insights Ricardo Rodriguez	L'analyse malware via l'IA Gledis Shkurti
15:20	30'	Backdoor sophistiquée GNU/Linux Théo Letailleur	Retex sur l'opération de désinfection de PlugX Worm Charles Meslay
15:50 - 16:20	30'	PAUSE	
16:20	30'	Qualifier l'ambigu : défis techniques et éthiques de qualification de malware Sylvio Hoarau	Reverse engineering d'une attaque : preuves, limites et actions prioritaires pour les institutions publiques Thomas Schaal
17:00	30'	Analyse dynamique à l'épreuve de l'évasion : plateforme, bacs à sable et limites Dorian Bachelot	En cours CCI Vaucluse
17:40	30'	Retour d'expérience sur 10 ans de comparaisons à large échelle de codes malveillants Tristan Pourcelot	
18:10	50'	RAFRAÎCHISSEMENTS (SANS ALCOOL)	

ÉCOLE DE L'AIR & DE L'ESPACE SALON-DE-PROVENCE · CCI VAUCLUSE · CCI INFORMATIQUE & DIGITAL · formind · orange Cyberdefense

Feed back - Cyb’Air Sud 2025

- **Trust me i’m a shortcut :**

  Les raccourci « bureau » sous windows

- **Analyse de malware avec r2ai et mcp (Personnel Fortinet)**

  10000 malwares par jour à identifier et traiter : goodware ou malware

  1 à 2h par malware

  Utilisation de l’IA pour dégrossir le chantier et extraire du code, notamment pour traiter l’obfuscation

  (déf : stratégie de gestion de l'information qui consiste à obscurcir le sens qui peut être tiré d'un message)

- **Détection comportementale des activités disque des Ransonwares et Génération de données synthétiques pour Anticiper les attaques futures…**

- **Du SOC au CERT : ce que le reverse engineering de malwares apporte vraiment**

- **Analyse OS android :**

  immense air de jeu pour les Malware, analyse du code

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

Feed back - Cyb’Air Sud 2025

- **The Kill chain for Android Malware : Delivery**
- **Vshell : The V stands for verbose**
- **Malware craftsmanship**
- **Malware Operations Under the Microscope : from binary Artifacts to strategic Insights**
- **Retex sur l’opération de désinfection de PlugX Worm**
- **Qualifier l’ambigu : defit techniques et éthiques de qualification de malware**
- **Analyse dynamique à l’épreuve de l’évasion : plateforme, bacs à sable et limites**
- **Retour d’expérience sur 10 ans de comparaisons à large échelle de codes malveillants**

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

Feed back - Cyb’Air Sud 2025

Malware : définition

- Les logiciels malveillants sont tout programme ou logiciel informatique conçu à des fins malveillantes.
- Les logiciels malveillants sont utilisés pour voler des données ou infliger des dommages aux systèmes informatiques ou logiciels.
- Les logiciels malveillants comprennent divers types de cybermenaces tels que les virus, les logiciels publicitaires, les logiciels espions et les ransomwares.
- Le plus souvent, l’objectif des cyberattaques est d’utiliser le malware pour un gain financier.

Feed back - Cyb’Air Sud 2025

Malware : quelques symptômes pour l’utilisateur sur leurs équipements

- Un ordinateur lent qui ralentit la vitesse Internet et les applications logicielles.
- La machine/l’appareil tombe fréquemment en panne ou se fige lors d’une utilisation normale.
- Une tonne de publicités contextuelles, indiquant des logiciels publicitaires. En cliquant sur ces publicités, vous pouvez lancer un code malveillant qui cause d’autres dommages.
- Une perte d’espace disque. Une perte soudaine d’espace disque disponible peut résulter d’un malware sur le disque dur.
- Une augmentation de l’activité Internet qui n’est pas corrélée au comportement des utilisateurs peut se produire lorsque les logiciels malveillants accèdent automatiquement à Internet.
- Un système surchargé en raison de malwares qui mobilisent des ressources précieuses.
- De nouvelles barres d’outils, extensions et une page d’accueil différente ou un site Web frauduleux où le malware a redirigé le navigateur.

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

Feed back - Cyb’Air Sud 2025

Malware : Différents types de logiciels malveillants

1. Virus
2. vers
3. Virus trojan
4. Logiciels espions
5. Ransomware
6. Logiciels publicitaires
7. Rootkit
8. Enregistreurs de frappe
9. Cryptojacking
10. Logiciel indésirable
11. Épouvantail

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

Feed back - Cyb’Air Sud 2025

Malware : Méthodes d’attaques par malware

- Les appareils non sécurisés
- Les réseaux non sécurisés
- Les dispositifs plus anciens
- Les pièces jointes aux e-mail
- Les e-mails de phishing ou de spear phishing
- Les SMS
- Les serveurs de fichiers
- Un logiciel de partage de fichiers
- Le partage de fichiers entre pairs (P2P)
- Les vulnérabilités réseau exploitables à distance

Le 28/11/2025 Jean-Charles GHATA, Floren PIANETTI, Lionel VEYAN

CyberDico :
https://cyber.gouv.fr/le-cyberdico

Malware d’après Fortinet :
https://www.fortinet.com/fr/resources/cyberglossary/malware

Cyb’Air sud 2025
https://cybair-sud.fr/pages/ed_2025.html