

# Une vaste panoplie de modes opératoires

Le Clusir Paca a organisé le 6 mars, en partenariat avec le Conseil régional de l'ordre des experts-comptables Marseille Paca et la Compagnie régionale des commissaires aux comptes Aix-Bastia, un atelier passionnant mais effrayant sur le thème « Les nouveaux modes opératoires cybercriminels ». Joffrey Boloni, RSSI à la société Sidesecurity.io, a exposé le sujet afin de mieux en appréhender et en comprendre les arcanes. Explications.

Aujourd'hui, la cybercriminalité devient un fléau très préoccupant. Les groupes cybercriminels changent leurs habitudes et tendent vers la décentralisation des services. En utilisant des technologies décentralisées, ils échappent ain-

Joffrey Boloni, Responsable de la sécurité des systèmes d'information (RSSI) à la société Sidesecurity.io, a évoqué les nouvelles approches et les cibles de choix. « Au départ, un simple constat : la multiplication des cibles par rapport à ce qui existait auparavant. »

si au blocage et à la censure. Fort de ce constat, les inquiétudes émergent chez les chefs d'entreprises, victimes potentielles. Aussi le Clusir Paca (Club de la sécurité de l'information région Provence-Alpes-Côte d'Azur) a souhaité exposer, en partenariat avec l'Ordre des experts-comptables Marseille Paca et la Compagnie régionale des com-

missaires aux comptes Aix-Bastia, les nouveaux modes opératoires cybercriminels afin de mieux expliciter aux professionnels les enjeux. « Le Clusir Paca, qui fédère plus de deux cents professionnels de la sécurité de l'information et les directeurs métiers intéressés, est sensible à l'acuité du sujet », a rappelé préalablement Me Alexandra Barberis, l'une de ses responsables.

En prélude à l'exposé, Joffrey Boloni, Responsable de la sécurité des systèmes d'information (RSSI) à la société Sidesecurity.io, a évoqué les nouvelles approches et les cibles de choix. « Au départ, un simple constat : la multiplication des cibles par rapport à ce qui existait auparavant. » Des menaces pèsent aujourd'hui sur le cryptosystème. Plus d'un milliard de dollars ont été détournés en 2018 sur différentes plateformes. Les attaques les plus simples, comme les « giveaways »\*, aux plus complexes ont été perpétrées. « Ce sont les attaques classiques des plateformes d'échange et des personnes, comme les plus discrètes avec les cryptomineurs. » Puis il a mentionné l'utilisation perverse des montres connectées : « Par le biais de recoupements, il est possible d'assurer l'exploitation de données publiques, de cartographier des sites sensibles comme des bases militaires », a-t-il confié.

## DÉTOURNEMENTS DE FONDS

Autre type d'attaque, sur les véhicules connectés. Le clonage des clés Tesla\*\* s'effectuent en quelques secondes pour



quelques centaines de dollars d'équipement. Autres moyens, les nouvelles techniques de déchiffrement avec un intermédiaire entre l'agresseur et la victime, ou encore la fraude au président. Le groupe Pathé en avait fait amèrement les frais avec un coût de 19 milliards d'euros.

Autre constat, les banques sont toujours une source de convoitises. La preuve : une cyberattaque Darkvihnaya impactant huit banques de l'Est. La méthode est simple : une personne fait une intrusion dans une banque en se faisant passer pour un candidat. Elle connecte un équipement malveillant au réseau de la banque et explore à distance son infrastructure IT. Elle installe des malwares, permettant d'orchestrer des braquages et de voler des fonds sur les comptes des banques. Autre exemple tangible : un virus faisant écran de fumée pour détourner l'attention de transactions frauduleuses lancées sur le réseau swift de la seconde banque chilienne qui accuse une perte de 10 M€. Joffrey Boloni a encore mentionné les distributeurs de billets pris pour cible dans une attaque coûtant 12 M€ à Cosmos Bank (Inde).

Dans un autre registre, se développent des formes de menaces plus personnelles. Des escrocs font croire aux in-

ternantes qu'ils possèdent des vidéos compromettantes.

Les habitudes des cybercriminels changent également avec l'éternel jeu du chat et de la souris. Une tendance à la décentralisation des services s'opère à présent. Les groupes cybercriminels quittent leurs plateformes traditionnelles. Des forums existent toutefois, le plus souvent hébergés dans des républiques membres du CIS\*\*\* (anciens Etats membres de l'URSS) et bénéficiant d'un certain niveau d'impunité. En clôture, Joffrey Boloni a conclu par ces propos : « Les cybercriminels restent maîtres pour retourner les moyens, les solutions et les outils à leur avantage. Aujourd'hui, c'est la blockchain. Et demain, l'intelligence artificielle ? »

Jean-Pierre Enaut  
jpenaut13@gmail.com

\* Les arnaques aux faux « giveaways » (donations) ont envahi les comptes Twitter des projets blockchain. De manière générale, il s'agit d'usurpateurs qui espèrent tirer profit de la ressemblance entre leur pseudonyme et le compte officiel d'un crypto-projet bien connu, en demandant l'envoi d'un certain montant en cryptomonnaies vers une adresse, tout en promettant de donner bien plus en échange.

\*\* Tesla est un constructeur automobile de voitures électriques dont le siège social est à Palo Alto (Etats-Unis), en Californie, dans la Silicon Valley.

\*\*\* Commonwealth of Independent States (CIS), en français Communauté des Etats indépendants.

De g. à dr., Guillaume Faure-Brac, président de la commission Numérique et innovation du Croec Paca, Christelle Dorison-Fourquet, présidente de la commission Intelligence économique et cybercriminalité des entreprises à la CRCC Aix-Bastia, Joffrey Boloni, RSSI à la société Sidesecurity.io, Me Alexandra Barberis du Clusir Paca, Matthieu Capuono, expert-comptable, directeur de Ficorec, past-président du CJD, et Hélène Trebosc-Campillo.