Pressemitteilung

Zur sofortigen Veröffentlichung Februar 2022

Cyberkriminalität bekämpfen: Menschliche und technische Ursachen verstehen

Ausgearbeitet von der Hochschule für den öffentlichen Dienst in Bayern, Fachbereich Polizei, in Kooperation mit Evangelos Markatos und Alexey Kirichenko im Auftrag des CC-DRIVER-Konsortiums

Dreizehn Partnerorganisationen aus der gesamten EU haben sich im Rahmen des mit 5 Mio. EUR finanzierten CC-DRIVER-Projekts zusammengeschlossen, um die menschlichen und technischen Ursachen von Cyberkriminalität zu untersuchen und neue Methoden zur Prävention, Ermittlung und Bekämpfung von cyberkriminellen Verhalten zu entwickeln.

Das Projekt konzentriert sich insbesondere auf Cybercrime-as-a-Service (CaaS), ein organisiertes Geschäftsmodell für die "Beauftragung" von Cyberkriminellen zur Erbringung illegaler Dienstleistungen oder für den Erwerb von Hilfsmitteln, Informationen und Fachwissen, die cyberkriminelle Operationen erleichtern. Zu diesen illegalen Dienstleistungen gehören das Hacken von Konten, Angriffe auf Konkurrenten und Geldwäsche, während Malware, Botnets und Informationen über Sicherheitslücken Beispiele für die Werkzeuge und Ressourcen sind, die über CaaS erworben werden können. CC-DRIVER hat gerade einen Bericht über CaaS in Europa veröffentlicht.

Cybercrime-as-a-Service ist ein wichtiges Geschäftsmodell, das Internetkriminalität vorantreibt: Eine neue Generation aufstrebender (Cyber-)Krimineller kann Ressourcen für Cyberkriminalität verkaufen, anstatt die wesentlichen Straftaten selbst begehen zu müssen, was Risiken verringert und ihre Gewinne erhöht. Auf der anderen Seite können Kriminelle ohne technische Kenntnisse illegale Cyberoperationen von erfahrenen Hackern einkaufen.

Der neue CC-DRIVER-Bericht "Landscape study of Cybercrime-as-a-Service" konzentriert sich auf ein breites Spektrum krimineller Aktivitäten, die im Rahmen

von Cybercrime-as-a-Service angeboten werden, wie z.B. Kryptowährungswäsche und -tumbling, Bulletproof Hosting, Hacking-as-a-Service, Distributed-Denial-of-Service (DDoS)-Angriffe, Spamming und Social Boosters. Außerdem werden aktuelle Trends in der Landschaft der Internetkriminalität untersucht, wie Servicemodelle, Kommunikationsmethoden und Wertschöpfung.

"Cybercrime-as-a-Service hat zu einer Ära der Industrialisierung der Internetkriminalität geführt", sagt der Mitverfasser des Berichts, Evangelos Markatos, Professor für Informatik und Leiter des Labors für verteilte Rechensysteme und Cybersicherheit am FORTH Institut für Computersicherheit. "Cyberkriminalität ist ein wachsendes Geschäft mit neuen Akteuren und Gruppen, die beständig auftauchen, mit neuen Marktplätzen, die im Darknet entstehen und alte ersetzen und die Entdeckung dieser Aktivitäten erschweren, und mit neuen Diensten und Produkten, die sich gegen neue Verteidigungsmaßnahmen richten. Ob es sich nun um Ransomware-as-a-Service, DDoS-Attacken-as-a-Service, Tumbling mit Kryptowährungen oder einen anderen Dienst handelt, eines ist klar: Cybercrime-as-a-Service ist heute Realität und wird sich weiter ausbreiten, solange es eine Nachfrage danach gibt."

Der vollständige Bericht "Landscape study of Cybercrime-as-a-Service" kann kostenlos unter https://www.ccdriver-h2020.com/deliverables heruntergeladen werden.

Das CC-DRIVER Konsortium

Das Projekt wird von David Wright, Trilateral Research (UK), koordiniert. Zu den weiteren Konsortialpartnern gehören F-Secure (Finnland), FORTH (Griechenland), Simavi (Rumänien), die Regionalpolizei von Valencia (Spanien), Policia Judiciária (Portugal), the School of Criminal Science an der Universität von Lausanne (Schweiz), KEMEA (Griechenland), die Hochschule für den öffentlichen Dienst in Bayern (Deutschland), die University of East London (UK), das Information Security Forum (UK), PrivaNova (Frankreich) und die griechische Polizei (Griechenland).

Weitere Informationen finden Sie unter https://www.ccdriver-h2020.com/consortium.

Bei Fragen wenden Sie sich bitte an

Evangelos Markatos, FORTH
markatos@ics.forth.gr

Das CC-DRIVER-Projekt – Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour [Ursachen von Cyberkriminalität verstehen und neue Methoden zur Prävention, Ermittlung und Bekämpfung von cyberkriminellem Verhalten entwickeln] – wird im Rahmen des H2020-Programms der Europäischen Union unter der Zuwendungsvereinbarung Nummer 883543 gefördert.